

– нові способи і засоби загоризонтного керування БПЛА з використанням функціонально спеціалізованої ПТП, включаючи можливість віддаленої корекції чи зміни польотного завдання з пункту наземного керування безпосередньо під час польоту БПЛА;

– нові компоненти системи аеромоніторингу на основі серійного БПЛА чи квадрокоптера і наземної підсистеми збору, обробки та накопичення моніторингової інформації та проведені випробування системи;

– нові алгоритми та програмні продукти по загоризонтному пілотуванню, по первинній обробці моніторингових даних, по накопиченню, індексації та збереженню даних;

– методичні рекомендації по проведенню випробувань та ефективному використанню систем моніторингу наземних об'єктів на основі безпілотних аеромобільних засобів з використанням ПТП.

Проведений ряд переваг безпілотних літальних апаратів перед пілотованими, дає можливість надати рекомендації щодо вибору оптимальних моделей БПЛА та систем управління для виконання задач щодо моніторингу наземних об'єктів.

Варіант використання БПЛА для передачі даних між наземним центром управління та базовим блоком системи моніторингу, а також структура компоновки БПЛА з роботизованим пристроєм, які наведені в статті, пропонується також вважати базовими при виборі оптимальних моделей БПЛА.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Класифікація UVS International [Електронний ресурс]. Режим доступу: <http://helpiks.org/6-70010.html>.
2. Büchi R. Faszination Quadrocopter. 1. Auflage. Verlag für Technik und Handwerk / R. Büchi. Verlag f.Technik / Handwerk, 2010. – 72 p. – ISBN 978-3-88180-791-3.
3. Riegler T. Quadrocopter richtig einstellen und fliegen / T. Riegler. Franzis, Poing 2011. ISBN 978-3-645-65073-1.
4. Rattat C. Multicopter selber bauen: Grundlagen –Technik – eigene Modelle / C. Rattat. Verl., Heidelberg, 2015. – ISBN 978-3-86490-247-5.
5. DronePort [Електронний ресурс]. – Режим доступу: <http://droneport.com.ua>.
6. Haas E. Aeronautical channel modeling / E. Haas // IEEE Transactions on Vehicular Technology. 2012. V. 51. № 2. P. 254-264.
7. Richard V.N. OFDM wireless multimedia communication / V.N. Richard, R. Prasad // Artech House Boston London. 2010. P. 260.

#### **ЛЕОНТЬЄВА Л. В.**

кандидат юридичних наук, доцент, старший викладач кафедри підготовки офіцерів запасу Національного юридичного університету імені Ярослава Мудрого

#### **КОЗАК МАРКО ІВАНОВИЧ**

студент 3 групи 2 курсу кафедри підготовки офіцерів запасу Національного юридичного університету імені Ярослава Мудрого

### **СУЧАСНІ ПІДХОДИ ТА ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ**

У нинішніх умовах, коли глобальні та регіональні виклики стають дедалі гострішими, питання забезпечення державної безпеки виходить на передній план, набуваючи пріоритетного значення для сталого розвитку суспільства і захисту національних інтересів. Сьогодні вимагає перегляду традиційних концепцій у формуванні системи безпеки,

оскільки характер загроз зазнає швидких і суттєвих змін. До таких нових форм небезпеки належать зокрема зростання гібридних війн, поширення інформаційного впливу з використанням маніпулятивних технологій, а також інтенсифікація кіберзлочинності — всі ці чинники потребують створення нових, адаптивних і проактивних стратегій протидії.

На мій погляд, ефективна сучасна політика у сфері безпеки повинна базуватися на трьох ключових принципах: системності, що гарантує врахування комплексного характеру загроз і включення усіх необхідних механізмів протидії; гнучкості, яка забезпечує здатність оперативно реагувати на мінливість ситуації; та випереджувальному реагуванні, що дозволяє не лише відповідати на ризики, але й передбачати їхній розвиток та запобігати негативним наслідкам.

У цьому контексті варто згадати також думку В. П. Горбуліна, який наголошує на тому, що сучасні процеси у сфері безпеки супроводжуються суттєвим зростанням ролі гібридних загроз. Ці загрози проявляються у інтегрованому використанні воєнних, політичних, економічних та інформаційних інструментів для досягнення недобросовісних цілей [1]. Таким чином, лише всебічний підхід, що об'єднує зусилля всіх сфер життєдіяльності держави, може забезпечити ефективне протистояння новим викликам сучасної епохи.

Я переконаний, що саме багатогранний і комплексний характер сучасних загроз вимагає не лише інтеграції різноманітних складових державного управління у сфері безпеки, а й значного підвищення рівня координації між ними для забезпечення ефективної взаємодії. Такий підхід сприяє формуванню системи, здатної оперативно реагувати на нові виклики та ризики. Особливого значення в цьому контексті набуває активне впровадження інноваційних технологій у механізми забезпечення державної безпеки. Технологічний прогрес відкриває як унікальні можливості, так і створює потенційні загрози, які кардинально змінюють динаміку функціонування національних інститутів.

Згідно з аналізом О. С. Власюка, цифрове середовище стало невід'ємним елементом сучасної державності, яке не лише сприяє модернізації управлінських процесів, але й породжує низку нових викликів, що ставлять під загрозу національну безпеку [2]. Тому важливо ухвалити комплексний підхід до подолання таких проблем шляхом зміцнення технологічного середовища та стратегічного планування у сфері захисту інтересів держави.

Я вважаю, що використання сучасних інформаційно-аналітичних систем, технологій штучного інтелекту та великих даних дозволяє значно підвищити ефективність управлінських рішень у сфері безпеки та забезпечити своєчасне виявлення потенційних загроз.

Важливою складовою державної безпеки є кібербезпека. Як підкреслює В. М. Богуш, інформаційний простір стає ключовим полем протиборства, а захист інформаційних ресурсів є одним із пріоритетних завдань держави [3]. Ми вважаємо, що ефективна система кіберзахисту повинна включати не лише технічні засоби, але й організаційні, правові та освітні механізми, спрямовані на підвищення рівня цифрової грамотності населення.

Також, особливу увагу слід приділити вдосконаленню та розвитку стратегічних комунікацій, які виступають ключовим інструментом у забезпеченні державної безпеки. В умовах сучасної інформаційної війни надзвичайно важливим завданням є створення механізмів, що сприяють підвищенню стійкості громадян до дезінформаційних загроз та маніпулятивних впливів. Формування такого рівня захисту інформаційного середовища обумовлює необхідність запровадження ефективної комунікаційної політики держави, яка не лише зміцнює довіру населення до владних органів, але й допомагає консолідувати націю навколо важливих суспільних цінностей та ідей.

Окрім цього, варто звернути увагу на потребу активного залучення наукових установ і приватного сектору до співпраці з державними структурами в контексті забезпечення безпеки. Така інтеграція дозволяє отримати доступ до найновітніших технологій та інноваційних розробок, що безпосередньо впливають на підвищення ефективності заходів з охорони державного суверенітету. Водночас подібна взаємодія сприяє оптимізації використання ресурсів, відкриває нові можливості для поліпшення технологічного оснащення системи безпеки та формує більш системний підхід до вирішення актуальних викликів у цьому напрямку.

На мою думку, сучасні методи забезпечення державної безпеки мають базуватися на гармонійному поєднанні традиційних інструментів з інноваційними технологіями, акцентуючи увагу на активному розвитку системи кібербезпеки, посиленні стратегічних комунікацій та впровадженні ефективної міжсекторальної співпраці. Такий підхід сприятиме зміцненню загальної стійкості держави перед викликами сучасності, а також створить передумови для її стабільного та гармонійного розвитку в довгостроковій перспективі.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.
2. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : монографія. Київ : НІСД, 2016. 528 с.
3. Богуш В. М., Юдін О. К. Інформаційна безпека держави : підручник. Київ : МК-Прес, 2005. 432 с.

#### **ЛЮЛЬКА АНТОН СЕРГІЙОВИЧ**

курсант факультету ЗДБ, 214 навчальної групи,  
Київського інституту Національної гвардії України

#### **ГЕНЕРАТИВНИЙ ШІ У ПІДГОТОВЦІ ВІЙСЬКОВОСЛУЖБОВЦІВ НГУ ДО STANAG 6001**

Система іншомовної підготовки військовослужбовців Національної гвардії України (НГУ) дедалі більше орієнтується на забезпечення мовної сумісності з арміями держав-членів НАТО, а отже і на досягнення стандартизованого мовного профілю за STANAG 6001. У документі ATrainP-5 мовну компетентність визначено як загальну здатність до мовної комунікації, а рівні володіння мовою поділено на шість рівнів – від 0 до 5 [5, р. 1–1]. Це робить стандарт не лише інструментом оцінювання, а й методичним орієнтиром для проектування змісту навчання.

Актуальність проблеми посилюється тим, що підготовка до STANAG 6001 у військовому середовищі відбувається в умовах обмеженого часу, службового навантаження, ротаций і потреби швидко підтримувати набутий рівень. М. І. Левко та М. О. Торська слушно зауважують, що тест STANAG 6001 «виконує не лише функцію контролю рівня володіння мовою, а й чинить регулятивний вплив» на зміст, структуру та методи навчання [1, с. 151].

У сучасній науковій літературі генеративний штучний інтелект розглядають як важливий ресурс мовної освіти, але не як повну заміну викладача. За висновком З. Венга та Ю. Фу, GenAI (генеративний ШІ) може «підвищити мотивацію та впевненість студентів» завдяки оперативному зворотному зв'язку та створенню залучальних навчальних матеріалів [6, с. 395]. Водночас автори наголошують на потребі враховувати ризики, пов'язані з приватністю даних, алгоритмічними упередженнями та нерівним доступом до технологій [6, с. 396, 414–415].

С. А. Чапель визначає чотири ключові напрями, на які вже впливає генеративний ШІ: мовна педагогіка, мовне оцінювання, засвоєння другої мови та підготовка викладача [2]. У цьому контексті йдеться не лише про автоматичну генерацію вправ, а й про переосмислення фідбеку, взаємодії, оцінювання та технологічно-педагогічної компетентності викладача. Огляд Л. Лова також показує, що попри швидке поширення GenAI у мовному навчанні, галузь і далі потребує більшої кількості емпіричних досліджень, чітких етичних рамок і виваженої інтеграції інструментів у навчальну практику [3].

Результати інших оглядових праць підтверджують цю тенденцію. Наприклад, Б. Лі та ін. узагальнюють, що ChatGPT уже використовується для підтримки самостійного навчання, генерації контенту та оптимізації окремих викладацьких процедур, однак дослідницьке поле досі характеризується перевагою короткотермінових і переважно вищоосвітніх кейсів [4].

Метою цього дослідження є уточнення потенціалу генеративного ШІ в підготовці військовослужбовців НГУ до тестування за стандартом STANAG 6001 та визначення