НАЦИОНАЛНА СИГУРНОСТ

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ И ДРОНОВЕТЕ В СЕКТОРА ЗА СИГУРНОСТ: НОВИ ВЪЗМОЖНОСТИ И КИБЕРРИСКОВЕ

ПЕТЪР ЙОРДАНОВ
НАЦИОНАЛНА СПОРТНА АКАДЕМИЯ „ВАСИЛ ЛЕВСКИ“
СОФИЯ, БЪЛГАРИЯ
11PETARYORDANOV@GMAIL.COM



Петър ЙОРДАНОВ *е доктор и главен асистент в НСА „Васил Левски“. Научните му интереси са в областта на киберсигурността и изкуствения интелект. ORCID: 0009-0002-5509-4334.*

Резюме: *Чрез анализ на публикации и документи на ЕС, НАТО и EASA статията систематизира киберрисковете при дроновете с изкуствен интелект, свързва ги с мерки за защита и обосновава ролята на подготовката на операторите.*

Ключови думи: *изкуствен интелект, дронове, безпилотни летателни апарати, киберсигурност, национална сигурност, GNSS, подготовка на оператори*

ARTIFICIAL INTELLIGENCE AND DRONES IN THE SECURITY SECTOR: NEW OPPORTUNITIES AND CYBER RISKS

PETAR YORDANOV
NATIONAL SPORTS ACADEMY "VASSIL LEVSKI", SOFIA, BULGARIA

Abstract: *Based on publications and EU, NATO and EASA documents, the article systematises the cyber risks of AI-enabled drones, links them to countermeasures and argues for operator training.*

Key words: *artificial intelligence, drones, unmanned aerial vehicles, cybersecurity, national security, GNSS, operator training*

УВОД

Дроновете вече не са технологична новост, а обичаен инструмент на полицията, армията, граничната охрана и службите за защита при бедствия. Същевременно те се превърнаха и в източник на заплахи. През септември 2025 г. летище Копенхаген беше затворено за около четири часа заради големи дронове в близост до него, а засегнатите пътници бяха около 20 000 [1]. Месец по-късно Европейската комисия и върховният представител на ЕС включиха Европейската инициатива за защита от дронове сред първите флагмански проекти в пътната карта за отбранителна готовност до 2030 г. [2].

Успоредно с това в дроновете навлиза изкуственият интелект (ИИ). Той разкрива нови възможности, но създава и уязвимости. Целта на статията е да систематизира какво добавя ИИ към дроновете в сектора за сигурност, какви киберрискове възникват и как могат да бъдат ограничени. Методът е документален анализ на научни публикации, документи на ЕС, НАТО и Агенцията на ЕС за авиационна безопасност (EASA) и публично описани случаи, като рисковете са групирани по засегнатия компонент и съпоставени с мерки.

1. КАКВО ДОБАВЯ ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ

Класическият дрон е по същество „летяща камера“, която бързо осигурява информация от труднодостъпни или опасни места. Изкуственият интелект разширява тази роля в три посоки.

Първата е автономната навигация. Дронът поддържа курс и заобикаля препятствия чрез собствените си сензори, без да зависи изцяло от сигнала на глобалната навигационна спътникова система (GNSS) и от връзката с оператора. Войната в Украйна показа колко важно е това при радиоелектронно противодействие. Според доклад на Центъра за стратегически и международни изследвания (CSIS) автономната навигация с ИИ е повишила дела на успешните удари от около 10-20% до около 70-80%, като решението за поразяване остава при човека [3]. Подобни данни трябва да се приемат критично. Проверка на публичните данни за баражиращите боеприпаси в същата война показва, че нито едно от осемте проверени твърдения за ефективността и употребата им не е потвърдено [4].

Втората посока е разпознаването на обекти. Машинното зрение открива в реално време хора, превозни средства или огнища на пожар. Lygouras и колектив например описват автономен дрон, който сам открива плуващ човек в открити води чрез обработка на изображението на борда и е проектиран да му пусне спасителен пояс [5].

Третата посока е анализът на данни. ИИ обобщава видео и сензорна информация в готова картина на обстановката. При масови спортни и обществени събития това позволява по-ранно откриване на опасни струпвания и инциденти [6]. Колкото повече обаче дронът „решава“ сам, толкова по-висока е цената на грешката, когато ИИ бъде подведен или навигацията бъде компрометирана.

2. КИБЕРРИСКОВЕТЕ: КЪДЕ Е УЯЗВИМ „УМНИЯТ“ ДРОН

Дронът с ИИ е летяща компютърна система и наследява уязвимостите на всяка такава система - на радиовръзката, на навигацията, на софтуера и на данните [7]. Основните рискове и мерките за защита, обобщени от автора по [7-11], са в табл. 1.

Риск	Какво се случва	Мерки за защита
Заглушаване на GNSS	Загуба на позицията, отклонение или падане	Резервна навигация; ръчно управление от оператора
Подмяна на GNSS сигнала	Дронът приема фалшива позиция	Сравняване на няколко източника на позиция
Прихващане на връзката	Изтичане на видео и данни, загуба на контрол	Криптиране; процедури при прекъсване
Подвеждане на ИИ	Пропусната цел или фалшива тревога	Човешка проверка на важните решения
Достъп до софтуера	Промяна на задачата, изтичане на данни	Обновяване; контрол на достъпа

Таблица 1. Основни киберрискове при дроновете с изкуствен интелект и мерки за защита

Заглушаване и подмяна на сателитния сигнал. При заглушаването (jamming) дронът губи сигнала на GNSS, например GPS. При подмяната (spoofing) му се подават фалшиви сателитни сигнали и той изчислява грешна позиция, без това да е очевидно. EASA посочва, че подобни смущения засягат и района на Черно море, а подмяната се открива по-трудно и не веднага [8]. Изследователи от Тексаския университет в Остин показаха, че чрез подмяна на GPS сигнала може да се поеме частичен контрол над полета на дрон [9].

Прихващане на връзката. Незащитеният канал за управление и видео може да бъде подслушан, прекъснат или поет от трето лице [7]. Изтичането на видео от полицейска операция или на маршрута на охранявано лице е пряк риск за сигурността.

Подвеждане на изкуствения интелект. Thys и колектив показаха, че специално изработено цветно изображение, отпечатано и държано пред тялото, може да направи човека практически невидим за широко използван алгоритъм за откриване на хора [10]. За дрон, който автоматично търси хора, това означава пропусната цел.

Достъп до софтуера. Зловреден код в дрона или в наземната станция може да промени задача-

та или да изнесе данни [7], а автономните интелигентни агенти пораждат нов клас киберзаплахи [11].

3. ПОДГОТОВКАТА НА ОПЕРАТОРИТЕ КАТО ПЪРВА ЛИНИЯ НА ЗАЩИТА

Техническите мерки са необходими, но не са достатъчни. Когато сателитният сигнал изчезне или ИИ сгреши, първата линия на защита е подготвеният оператор.

Качев и колектив от ВВМУ „Н. Й. Вапцаров“ предлагат концепция за обучение на пилоти за реагиране при кризи чрез минидронове в закрити помещения, където сателитният сигнал липсва или е ненадежден [12]. Обучението включва четири практически модула: разузнаване и наблюдение, търсене и спасяване в закрито пространство, реагиране при наводнение и при химически разлив. Авторите подчертават, че пилотирането е необходимо, но не е достатъчно: възприемането и тълкуването на обстановката, картографирането, докладването и координацията са също толкова важни цели [12].

Този подход има стойност и за киберсигурността. Операторът, свикнал да лети без сателитен сигнал, вероятно по-трудно ще бъде изненадан от заглушаване. Предлага се към подобни програми да се добавят кратки сценарии с киберизмерение, задавани от инструктора или чрез симулатор:

- внезапна загуба на позицията по време на задача;
- несъответствие между показанията на навигацията и видимата обстановка;
- прекъсване или забавяне на видеовръзката;
- съмнителен резултат от автоматичното разпознаване, който трябва да бъде проверен от човек.

Така операторът се учи не само да управлява дрона, но и да се съмнява в машината, когато има основание. Подобни сценарии могат да бъдат включени в подготовката на служителите от МВР и Българската армия.

4. ПРЕПОРЪКИ

Въз основа на анализа се отправят следните препоръки към институциите от сектора за сигурност:

- **Сигурност още при закупуването.** Криптирането на връзката, резервната навигация и защитата от подмяна на сигнала да бъдат част от техническите изисквания в обществените поръчки за дронове.
- **Запазване на човешкия контрол.** Решенията с тежки последици да се вземат от човек. Принципите на НАТО за отговорна употреба на ИИ - законосъобразност, отговорност и отчетност, обяснимост и проследимост, надеждност, управляемост и намаляване на пристрастията - дават готова рамка за това [13].
- **Ясни правила.** Регламентът на ЕС за ИИ не се прилага за системи, използвани изключително за военни цели, отбрана или национална сигурност, но обхваща употребата им от полицията и граничната охрана [14]. Изключените системи трябва да бъдат уредени с национални и ведомствени правила.
- **Отчитане на инцидентите.** Смущенията в навигацията и опитите за прихващане да се докладват и анализират систематично, по подобие на подхода на EASA в гражданската авиация [8].
- **Редовно обучение.** Сценариите с киберизмерение да станат постоянна част от подготовката на операторите.

ЗАКЛЮЧЕНИЕ

Изкуственият интелект прави дроновете по-самостоятелни и по-полезни за сектора за сигурност, но и по-привлекателна цел. Заглушаването и подмяната на сателитния сигнал, прихващането на връзката и подвеждането на алгоритмите за разпознаване вече са демонстрирани на практика.

Приносът на статията е в три насоки: основните киберрискове при дроновете с ИИ са систематизирани по компоненти на системата и свързани с конкретни мерки; обоснована е ролята на операторите като първа линия на защита; предложено е обучението по концепцията на Качев и колектив да се допълни със сценарии с киберизмерение. Предстои практическата проверка на тези сценарии при обучението на служители от сектора за сигурност.

ЛИТЕРАТУРА

[1] Reuters. Drones that shut Copenhagen airport flown by „capable operator“, Danish police say. London: Reuters, 23.09.2025.

[2] European Commission, High Representative of the Union for Foreign Affairs and Security Policy. Preserving Peace - Defence Readiness Roadmap 2030. Joint Communication. Brussels: European Commission, 16.10.2025.

[3] K. Bondar. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare. Washington, DC: Center for Strategic and International Studies, 2025.

[4] И. Вълков. Верификация на данните за ефективността на баражиращите боеприпаси и предизвикателства пред придобиването им, Национална сигурност, Виктори Издат, бр. 28, 2026. https://nacionalna-sigurnost.bg/брой-28/

[5] E. Lygouras, N. Santavas, A. Taitzoglou, K. Tarchanidis, A. Mitropoulos, A. Gasteratos. Unsupervised Human Detection with an Embedded Vision System on a Fully Autonomous UAV for Search and Rescue Operations, Sensors, Basel: MDPI, Vol. 19 (16), 2019, 3542. DOI: 10.3390/s19163542.

[6] П. Йорданов. Приложение на изкуствен интелект за подобряване на сигурността при спортни и масови събития. Монография. София: НСА ПРЕС, 2026. ISBN 978-954-718-817-4.

[7] J.-P. Yaacoub, H. Noura, O. Salman, A. Chehab. Security analysis of drones systems: Attacks, limitations, and recommendations, Internet of Things, Amsterdam: Elsevier, Vol. 11, 2020, 100218. DOI: 10.1016/j.iot.2020.100218.

[8] European Union Aviation Safety Agency. Safety Information Bulletin SIB 2022-02R4: Global Navigation Satellite System Outage and Alterations Leading to Communication / Navigation / Surveillance Degradation. Cologne: EASA, 2026.

[9] A. J. Kerns, D. P. Shepard, J. A. Bhatti, T. E. Humphreys. Unmanned Aircraft Capture and Control via GPS Spoofing, Journal of Field Robotics, Hoboken: Wiley, Vol. 31 (4), 2014, 617 - 636. DOI: 10.1002/rob.21513.

[10] S. Thys, W. Van Ranst, T. Goedemé. Fooling Automated Surveillance Cameras: Adversarial Patches to Attack Person Detection, 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach: IEEE, 2019, 49 - 55. DOI: 10.1109/CVPRW.2019.00012.

[11] И. Савов. Агентният изкуствен интелект и бъдещето на киберсигурността - нов оперативен модел за противодействие на автономни киберзаплахи, Национална сигурност, Виктори Издат, бр. 26, 2026. https://nacionalna-sigurnost.bg/брой-26/

[12] O. Kachev, N. Velikov, T. Koritarov, G. Kalinov, N. Stoycheva, Y. Minkova. Concept for Training UAV Pilots for Crisis Response Using Mini-Drones in Indoor Environments, Морски научен форум, Варна: ВВМУ „Н. Й. Вапцаров“, Т. 11 (1), 2026. DOI: 10.63662/ardkm862.

[13] NATO. Summary of NATO's Revised Artificial Intelligence (AI) Strategy. Brussels: NATO, 2024.

[14] Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект (Акт за изкуствения интелект), Официален вестник на Европейския съюз, L, 12.07.2024.