

Т. В. Бібік

канд. техн. наук, доц.

Навчально-науковий інститут атомної та теплової енергетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Берестейський, 37, Київ, 03056, Україна

ORCID: 0000-0003-0134-6022

В. Г. Гончарук*Навчально-науковий інститут атомної та теплової енергетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Берестейський, 37, Київ, 03056, Україна*

ORCID: 0009-0007-9647-1462

Оцінка вразливості систем фізичного захисту до безпілотних літальних апаратів з оптоволоконним зв'язком

Ключові слова:

системи фізичного захисту,
атомні електростанції,
безпілотні літальні апарати,
оптоволоконний канал зв'язку,
радіоелектронна протидія,
законодавчі обмеження,
ядерна безпека,
вразливість критичної
інфраструктури,
протидія дронам,
організаційні та правові заходи

Розглянуто актуальну проблему виникнення нового типу загроз для систем фізичного захисту об'єктів критичної інфраструктури, пов'язану з використанням безпілотних літальних апаратів, що оснащені оптоволоконними каналами керування та передавання відеоінформації. Зазначено, що застосування оптоволоконного зв'язку суттєво змінює підходи до забезпечення безпеки, оскільки такі літальні апарати є практично нечутливими до традиційних засобів радіоелектронної протидії, які широко використовуються в сучасних системах фізичного захисту. Проаналізовано технічні та експлуатаційні переваги багатороторних безпілотних літальних апаратів з оптоволоконним керуванням у контексті подолання наявних бар'єрів фізичного захисту, зокрема можливість прихованого наближення до об'єкта, стійкість до радіоподавлення та забезпечення стабільного каналу керування в умовах складної електромагнітної обстановки. Окрему увагу приділено оцінюванню доступності комплектуючих елементів і технологій, необхідних для виготовлення таких апаратів у несанкціонованих або домашніх умовах, а також аналізу орієнтовних фінансових витрат на їх створення. Розглянуто ризики, які безпілотні літальні апарати з оптоволоконним зв'язком можуть створювати для безпечної експлуатації АЕС та інших об'єктів критичної інфраструктури, з урахуванням можливих сценаріїв використання їх зловмисниками. Запропоновано напрями удосконалення організаційних і правових заходів захисту, а також обґрунтовано доцільність внесення змін до законодавства України щодо обмеження доступу фізичних осіб до ключових компонентів, які можуть бути використані для створення оптоволоконних каналів керування безпілотними літальними апаратами.

Вступ

Зростання використання безпілотних літальних апаратів (БПЛА) створює нові виклики для систем

фізичного захисту критичних об'єктів, зокрема АЕС, аеропортів, стадіонів, складів або військових об'єктів. Традиційні методи боротьби з дронами передбачають застосування засобів радіоелектронної проти-

© Т. В. Бібік В. Г. Гончарук, 2026. Ліцензія CC BY 4.0

дії, що базуються на придушенні каналів управління та навігації. Однак поява концепції оптоволоконних БПЛА змінює ситуацію. Такі дрони отримують сигнали управління не через радіоканал, а через кабель оптоволоконна, що робить їх невразливими до традиційних методів придушення [1]. Це відкриває можливості для потенційних зловмисників створювати апарати з підвищеним рівнем стійкості до виявлення та нейтралізації.

Аналіз літературних даних та постановка проблеми

Наукова література щодо оптоволоконних БПЛА є обмеженою, проте питання використання альтернативних каналів управління активно обговорюється в публікаціях Інституту інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE) [2]. МАГАТЕ у своїх рекомендаціях із фізичного захисту вказує на необхідність урахування нових технологій, які можуть бути використані для обходу наявних систем захисту [3]. У НАТО в 2020–2022 рр. були проведені дослідження щодо методів боротьби з безпілотниками нового покоління, включно з автономними апаратами та апаратами із захищеними каналами управління. Зокрема, у звітах підкреслюється, що законодавчі заходи мають йти в ногу з технічним прогресом [4]. У країнах ЄС та США впроваджуються багаторівневі системи захисту критичної інфраструктури від БПЛА, що включають правові, організаційні та технічні заходи [5]. ЄС використовує концепцію U-Space та обов'язкову ідентифікацію Remote ID, що дає змогу відстежувати дозволені польоти та виявляти порушників у режимі реального часу [6]. У США аналогічні функції виконує система Remote ID, а також тимчасові обмеження польотів (TFR), які захищають критично важливі об'єкти [7].

Сучасні технології протидії безпілотникам поділяються на два класичні напрями — некінетичні засоби та кінетичні методи нейтралізації [8]. До некінетичних належать радіоподавлення каналів управління та GPS, радіоперехоплення, оптичне та радіочастотне виявлення. Кінетичні засоби включають системи стрільби сітками, інтерцептор-дрони, а також високоточні лазерні системи, що застосовуються переважно у військових умовах через юридичні обмеження [9]. Європейські держави впроваджують інтегровані системи, які поєднують радарні комплекси малої дальності, радіомоніторинг, акустичні сенсори та оптичні модулі в єдиний центр управління за-

грозами. У США значну роль відіграють агентства DHS та DoD, які сертифікують системи C-UAS і координують захист ядерних об'єктів та енергетичної інфраструктури [10]. Технології directed-energy, інтерцептор-дрони та системи знешкодження високоточними лазерами активно досліджуються для майбутнього застосування, але наразі мають обмеження через високу вартість і регуляторні вимоги [11]. Для захисту від БПЛА з оптоволоконним каналом зв'язку, які не реагують на радіоподавлення, особливого значення набувають багатосенсорні системи, а також фізичний захист критичних вузлів та стратегічних елементів інфраструктури [12].

Мета та завдання дослідження

Метою дослідження є розробка пропозицій щодо удосконалення законодавства України у сфері ядерної безпеки з метою запобігання використанню оптоволоконних БПЛА у злочинних цілях. Для досягнення цієї мети поставлено завдання:

- оцінити можливість створення оптоволоконних БПЛА в домашніх умовах;
- проаналізувати ризики для систем фізичного захисту (СФЗ) та експлуатації АЕС та інших критичних об'єктів;
- провести аналіз ринку деталей, інструменту та готових БПЛА;
- розглянути можливі негативні наслідки законодавчих обмежень;
- сформулювати пропозиції щодо організаційних та правових заходів.

Методика дослідження

Дослідження ґрунтується на аналізі вразливостей систем фізичного захисту АЕС та оцінюванні можливості виготовлення оптоволоконних БПЛА в несанкціонованих умовах. Було розглянуто технічні характеристики БПЛА на оптоволоконні, доступність його придбання на ринку, а також варіанти використання його як засобу зв'язку між оператором та дроном. Окремо досліджено сценарії потенційних атак і заходи протидії, які можуть застосовуватись у рамках чинного законодавства.

Результати дослідження

Для виготовлення БПЛА на оптоволоконній системі керування в домашніх умовах потрібно вивчи-

ти інформацію та мати необхідні деталі. Короткий список основних компонентів є таким: міцна та достатньо легка рама, зазвичай з карбонового волокна, а також достатньо велика, щоб нести корисне навантаження; двигуни та регулятори обертів із запасом потужності, достатнім для забезпечення польоту з урахуванням повної маси; пропелери; польотний контролер; акумуляторна батарея; камера; оптоволоконний кабель.

Також необхідні допоміжні інструменти та обладнання, зокрема: паяльник або паяльна станція; набір ручного інструменту (викрутки, пінцети, кусачки, плоскогубці); 3D-принтер (опціонально); сколювач оптоволоконна, призначений для підготовки волокна до зварювання з метою мінімізації втрат сигналу, що є критично важливим на великих дистанціях; зварювальний апарат для оптоволоконна.

Такий набір деталей та інструментів на ринку України коштує щонайменше 24 000 грн, якщо брати середню якість — це вже 131 000 грн, враховуючи зварювальний апарат, це найдорожчий інструмент, а якщо користуватись преміальними деталями та професійним інструментом, то ціна одного БПЛА може сягати й мільйона гривень, з тепловізійною камерою, стабілізатором, додатковою периферією та ін.

У той же час аналіз ринку показав, що готовий дрон можна придбати за 28 000 грн, причому така покупка є доступною практично для будь-кого.

Було встановлено, що сучасне законодавство України не регламентує обіг оптоволоконна як потенційно небезпечного матеріалу. Фактично будь-яка фізична особа може придбати необхідні компоненти для створення системи управління дроном через оптоволоконний кабель. Водночас аналіз показав, що використання оптоволоконних каналів робить дрони стійкими до традиційних методів придушення сигналів. Це створює нову категорію загроз для СФЗ та експлуатації АЕС.

Обговорення ризиків

Основні ризики, пов'язані з оптоволоконними БПЛА:

неможливість застосування стандартних засобів радіоелектронної боротьби;

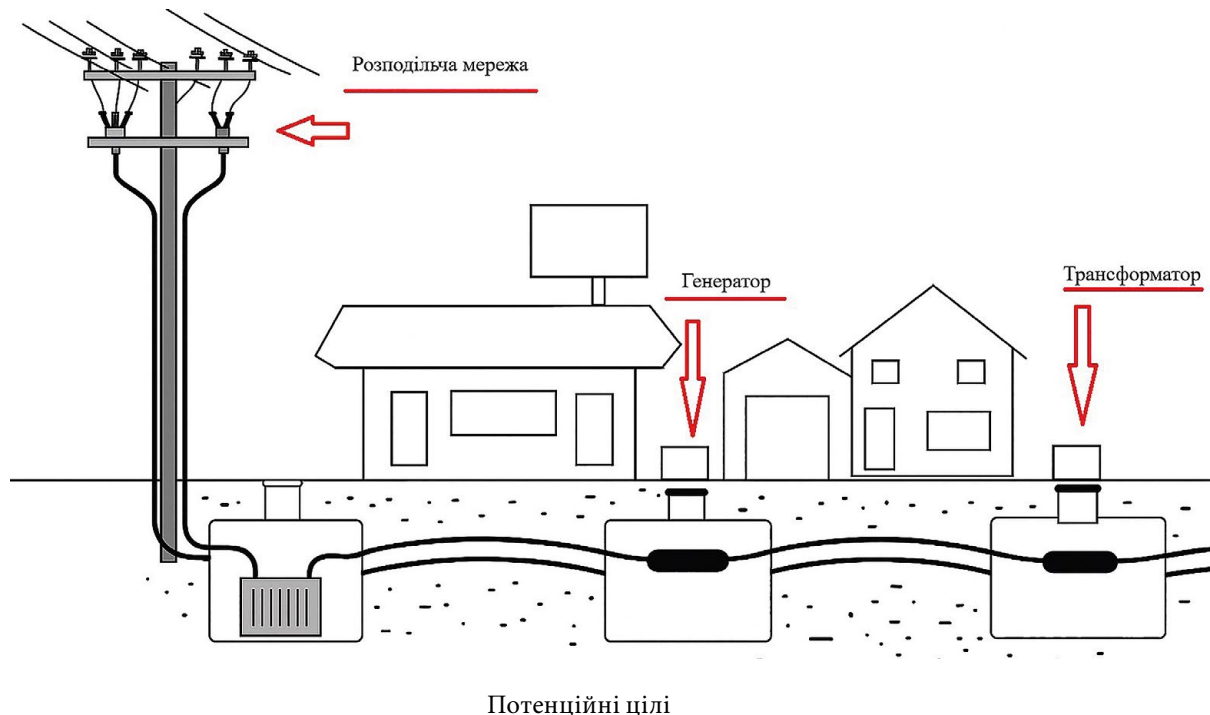
відсутність випромінюваного сигналу, що ускладнює виявлення безпілотної;

можливість доставлення небезпечних вантажів до периметра або навіть всередину АЕС;

використання оптоволоконних дронів для тривалого спостереження або диверсій;

підвищення складності виявлення таких пристроїв традиційними сенсорами.

Ціллю дрона можуть бути як незначні об'єкти інфраструктури (рисунок), зокрема трансформатори біля житлових будинків, генератори та елементи мережі електропередачі, так і великі дороговартісні



об'єкти, наприклад силові трансформатори на ТЕЦ або АЕС, паливні цистерни, літаки чи їхні критично важливі агрегати.

Відповідно, і ціна такої атаки може варіюватися від тисяч до мільйонів чи навіть мільярдів гривень.

Можлива атака на відкриті розподільчі пристрої, трансформатори, лінії електропередачі за допомогою дрона-камікадзе або дрона, що доставляє металеві предмети/засоби ураження. При цьому радіоканали придушення неефективні, а дрон залишається керованим через волоконний канал.

Доставка небезпечних/заражених матеріалів до периметра АЕС. Використання БПЛА для доставки радіаційно небезпечних, хімічних чи біологічних матеріалів у зону фізичного захисту (із зовні або за участі «внутрішнього порушника»). У такому сценарії оптоволоконний канал знижує ризик виявлення за допомогою радіомоніторингу.

Розвідка та коригування вогню. Безперервна розвідка периметра АЕС оптоволоконним дроном для виявлення схем патрулювання, технічних обмежень СФЗ, відстеження роботи персоналу, що може бути використано як для планування атак, так і для коригування вогню інших засобів ураження.

Аналіз можливих законодавчих змін

Пропонується внести до законодавства України норму, яка передбачає заборону фізичним особам придбання та зберігання оптоволоконна, яке може бути використане для виготовлення каналів управління БПЛА. Це знизить імовірність створення кустарних оптоволоконних дронів. Водночас подібна заборона може мати негативні наслідки, зокрема:

обмеження доступу для легальних користувачів (наприклад, компаній, що займаються телекомунікаціями);

необхідність створення механізмів контролю та ліцензування;

ризик виникнення чорного ринку.

Пропозиції рішень

1. Встановлення обов'язкового ліцензування операцій з оптоволоконком.

2. Впровадження системи обліку постачань та споживачів.

3. Створення спеціальних груп моніторингу для виявлення незаконного використання дронів та деталей для створення безпілотних систем.

4. Паралельний розвиток технічних засобів виявлення оптоволоконних БПЛА.

5. Проведення навчань персоналу охорони щодо реагування на подібні загрози, написання інструкцій для персоналу.

6. Огородження вразливих вузлів на території критичної інфраструктури та захист відповідно до їхньої значущості.

Приклади заходів в інших країнах

Велика Британія

Розгортання локальних C-UAS рішень біля аеропортів і критичних об'єктів (радар + RF детектування + оптичні засоби детектування).

Акцент на інтеграцію з поліцією й службою авіаційної безпеки.

Франція

Після кількох інцидентів із дронами над критичними об'єктами посилено законодавство щодо заборонених зон; існують мобільні системи перехоплення (використовують у поліції та армії).

Деякі приватні оператори інфраструктури впроваджують сервіси радіомоніторингу (Dedrone, DroneShield).

Нідерланди, Німеччина

Впровадження U-Space / Remote ID, розвиток офіційних процедур оповіщення та спільних тренувань між операторами АЕС/енергетики та правоохоронцями.

США

Перевірені програми DHS S&T та DoD з C-UAS технологіями; експериментальні розгортання лазерних систем та систем «інтерцептор-дронів», тобто дронів-перехоплювачів.

На федеральному рівні — сильний акцент на законність застосування: Only authorised entities may conduct kinetic/RF disruption.

Законодавчі рішення

Європа

Remote ID / U-Space: ЄС впроваджує систему U-Space/Remote ID, яка регламентує ідентифікацію та управління повітряним простором для дронів. Це дає змогу відстежувати зареєстровані БПЛА та визначати невідомі апарати.

Національні режими заборонених зон: держави вводять заборонені зони (no-fly zones) для дронів над критичною інфраструктурою; цивільні оператори мусять дотримуватися обмежень.

Правозастосування: право застосовувати заходи із технічної нейтралізації зазвичай надається поліції, військовим або спеціальним державним агентствам. Приватним власникам інфраструктури дозволено здебільшого лише пасивні заходи (огорожа, евакуація, оповіщення).

США

FAA Remote ID & TFR: Федеральна авіаційна адміністрація (FAA) зобов'язала виробників мати Remote ID, ввела механізми тимчасових обмежень польотів (TFR).

DHS/DoD/FBI: у разі загрози національній інфраструктурі у відповідь можуть бути залучені служби національної безпеки; існують програми сертифікованого застосування C-UAS (Counter-UAS).

Правові обмеження: знищувати або глушити сигнали дронів без дозволу заборонено — це стосується навіть глушіння в певних частотах (регулюється FCC).

Перспективи розвитку та подальші дослідження

Подальші дослідження мають бути спрямовані на: розробку технологій виявлення оптоволоконних дронів;

створення міжнародних стандартів регулювання обігу оптоволоконна;

аналіз ефективності організаційних і правових заходів;

оцінку впливу запропонованих змін на економіку та телекомунікаційну галузь.

Аналіз вказує на те, що поява оптоволоконних БПЛА є серйозним викликом для традиційних підходів у сфері фізичного захисту. З огляду на те, що ці технології не охоплюються чинними стандартами, їх регулювання має бути пріоритетним завданням держави. Міжнародний досвід демонструє, що своєчасне впровадження обмежень може суттєво знизити ризик використання новітніх технологій у злочинних цілях. Водночас слід забезпечити баланс між національною безпекою та інтересами легальних галузей, що використовують оптоволоконно у своїй діяльності.

Висновки

1. Виявлено нову категорію загроз для СФЗ та АЕС, пов'язану з використанням оптоволоконних каналів керування БПЛА.

2. Традиційні методи боротьби з дронами виявляються неефективними проти оптоволоконних систем.

3. Пропонується законодавчо обмежити доступ фізичних осіб до оптоволоконна з метою унеможливлення кустарного виготовлення таких дронів.

4. Запропоновано комплекс організаційних та правових заходів, включаючи ліцензування, контроль обігу та створення груп моніторингу.

5. Подальші дослідження мають зосереджуватися на технологічних рішеннях та міжнародній координації.

Європейський та американський досвід свідчить, що найбільш ефективним є комплексний підхід «система в системі», за якого технічні рішення поєднуються з чіткою нормативно-правовою базою та визначеними процедурами реагування. Існує значна кількість технологій нейтралізації БПЛА, але їх застосування має бути обмежене законом і вимагає ретельної оцінки ризиків. Для захисту від оптоволоконних БПЛА, які не реагують на засоби радіочастотного придушення, особливу увагу доцільно приділяти оптичним, акустичним і радарним засобам виявлення, а також фізичному захисту критично важливих елементів інфраструктури.

Список використаної літератури

1. Smith J. Alternative communication channels for unmanned aerial vehicles / J. Smith // IEEE Communications Magazine. – 2021. – Vol. 59, No. 6. – P. 48–54. – Available at: doi.org/10.1109/MCOM.001.2001234.
2. Clough B. Metrics, schmetrics: How the application of metrics can lead to dangerous UAV vulnerabilities / B. Clough // IEEE Aerospace and Electronic Systems Magazine. – 2021. – Vol. 36, No. 4. – P. 6–14. – Available at: doi.org/10.1109/MAES.2021.3053214.
3. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). – Vienna : International Atomic Energy Agency, 2019. – 87 p. – Available at: <https://www.iaea.org/publications/11007/nuclear-security-recommendations-on-physical-protection-of-nuclear-material-and-nuclear-facilities>.
4. Emerging Drone Threats and Countermeasures. – Brussels : NATO Science and Technology Organization., 2020. – 112 p. – Available at: <https://www.sto.nato.int/publications/STO%20Reports/Forms/AllItems.aspx>.
5. U-Space Regulatory Framework. Cologne: European Union Aviation Safety Agency, 2021. – Available at: <https://www.easa.europa.eu/en/domains/drones/u-space>.
6. Commission Implementing Regulation (EU) 2021/664 on a regulatory framework for the U-space // Official Journal of the European Union. – 2021. – Available at: https://eur-lex.europa.eu/eli/reg_impl/2021/664/oj.

7. Remote Identification of Unmanned Aircraft. Federal Aviation Administration. – Washington, 2023. – Available at: <https://www.faa.gov/uas/remote-id>.
8. Counter-Unmanned Aircraft Systems: Technology Overview. – Washington: U. S. Department of Homeland Security, Science and Technology Directorate, 2022. – Available at: www.dhs.gov/publication/counter-unmanned-aircraft-systems.
9. Sweetman B. Unmanned Aerial Vehicles and Cybersecurity / B. Sweetman – London: Routledge, 2020. – 214 p. – Available at: <https://doi.org/10.4324/9780429290121>.
10. Critical Infrastructure Drone Threat Assessment. – Washington: U. S. Department of Homeland Security, 2022. – Available at: <https://www.cisa.gov/resources-tools/resources/protect-2020>.
11. High Energy Laser Counter-Unmanned Aircraft Systems Trials Report. – Washington: U. S. Department of Defense, 2023. – Available at: <https://www.defense.gov/Newsroom/Reports>.
12. Finn A. Unmanned Aircraft Systems / A. Finn, D. Wright // Surveillance, Ethics and Privacy in Civil Applications. – Dordrecht : Springer, 2016. – 250 p. – Available at: <https://doi.org/10.1007/978-94-017-7784-8>.

ical protection barriers, including the possibility of covert approach to protected facilities, resistance to radio signal suppression, and the provision of a stable control channel under complex electromagnetic conditions. Particular attention is paid to the assessment of the availability of components and technologies required for the manufacture of such aerial vehicles in unauthorized or home environments, as well as to the analysis of approximate financial costs associated with their production.

The paper examines the risks that unmanned aerial vehicles with fiber-optic communication may pose to the safe operation of nuclear power plants and other critical infrastructure facilities, taking into account possible scenarios of their use by malicious actors. Directions for improving organizational and legal protection measures are proposed, and the feasibility of introducing amendments to the legislation of Ukraine aimed at restricting private access to key components that may be used to create fiber-optic control channels for unmanned aerial vehicles is substantiated.

Keywords: physical protection systems, nuclear power plants, unmanned aerial vehicles, fiber-optic communication channel, electronic countermeasures, legislative restrictions, nuclear security, critical infrastructure vulnerability, counter-UAV measures, organizational and legal protection measures.

T. V. Bibik, V. H. Honcharuk

Educational and Scientific Institute of Atomic and Thermal Power Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Beresteyskyi Ave, Kyiv, 03056, Ukraine

Assessment of the Vulnerability of Physical Protection Systems to Unmanned Aerial Vehicles with Fiber-Optic Communication

The article addresses the relevant problem of the emergence of a new type of threat to the physical protection systems of critical infrastructure facilities associated with the use of unmanned aerial vehicles equipped with fiber-optic channels for control and video data transmission. It is noted that the application of fiber-optic communication significantly changes existing security approaches, since such aerial vehicles are practically insensitive to traditional means of electronic countermeasures that are widely used in modern physical protection systems.

The technical and operational advantages of multi-rotor unmanned aerial vehicles with fiber-optic control are analyzed in the context of overcoming existing phys-

References

1. Smith J. (2021). Alternative communication channels for unmanned aerial vehicles. *IEEE Communications Magazine*, vol. 59 (6), pp. 48-54. Available at: doi.org/10.1109/MCOM.001.2001234.
2. Clough B. (2021). Metrics, schmetrics: How the application of metrics can lead to dangerous unmanned aerial vehicle vulnerabilities. *IEEE Aerospace and Electronic Systems Magazine*, vol. 36 (4), pp. 6-14. Available at: <https://doi.org/10.1109/MAES.2021.3053214>.
3. International Atomic Energy Agency (2019). *Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Revision 5)*. Available at: <https://www.iaea.org/publications/11007/nuclear-security-recommendations-on-physical-protection-of-nuclear-material-and-nuclear-facilities>.
4. NATO Science and Technology Organization (2020). *Emerging drone threats and countermeasures*. NATO STO. Available at: <https://www.sto.nato.int/publications>.
5. European Union Aviation Safety Agency (2021). *U-space regulatory framework*. Available at: <https://www.easa.europa.eu/en/domains/drones/u-space>.

6. European Commission (2021). Commission implementing regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space. *Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/eli/reg_impl/2021/664/oj.
7. Federal Aviation Administration (2023). Remote identification of unmanned aircraft. Available at: <https://www.faa.gov/uas/remote-id>.
8. U. S. Department of Homeland Security, Science and Technology Directorate (2022). *Counter-unmanned aircraft systems: Technology overview*. Available at: <https://www.dhs.gov/publication/counter-unmanned-aircraft-systems>.
9. Sweetman B. (2020). *Unmanned aerial vehicles and cybersecurity*. Routledge. Available at: <https://doi.org/10.4324/9780429290121>.
10. U. S. Department of Homeland Security (2022). *Critical infrastructure drone threat assessment*. Available at: <https://www.cisa.gov/resources-tools/resources/protect-2020>.
11. U. S. Department of Defense (2023). *High energy laser counter-unmanned aircraft systems trials report*. Available at: <https://www.defense.gov/Newsroom/Reports>.
12. Finn A., Wright D. (2016). *Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications*. Springer. Available at: <https://doi.org/10.1007/978-94-017-7784-8>.

Надійшла / Received 22.03.2026
Рекомендована до друку / Accepted 07.05.2026