http://doi.org/10.35668/2520-6524-2024-3-12
УДК 623.7

М. М. ДІВІЗІНЮК, д-р фіз.-мат. наук, проф.
О. В. ФАРРАХОВ, канд. техн. наук, пров. н. с.
Л. А. МАРЦЕВА, д-р пед. наук, доц.
А. О. КОЦЮБИНСЬКИЙ, канд. фіз.-мат. наук, доц.
О. В. ВЛАСЕНКО, ст. викладач

АНАЛІЗ СЦЕНАРІЇВ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРОТИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Резюме. *Мета статті полягає в аналізі використання безпілотних літальних апаратів у контексті гарантування безпеки об'єктів критичної інфраструктури. Для досягнення поставленої мети було вирішено наступні завдання. Спочатку було розглянуто проблему і поставлено задачу дослідження. Показано, що безпілотні літальні апарати становлять суттєву небезпеку для об'єктів критичної інфраструктури держави. На наступному етапі описано типові об'єкти критичної інфраструктури держави та взято для прикладу типову атомну електростанцію. Показано, що безпілотні літальні апарати мають широкий спектр типізації як за конструктивними особливостями, так і за класифікаційними ознаками. Здійснено аналіз та представлено можливі шляхи використання безпілотних літальних апаратів проти об'єкта критичної інфраструктури. Показано, що малі та середні безпілотні літальні апарати можуть використовуватися зловмисниками як розвідувальні, так і локально-ударні засоби ураження інфраструктури об'єкта критичної інфраструктури. Великі безпілотні літальні апарати можуть використовуватись як некеровані засоби ураження, так і як засоби підтримки дії диверсійних груп. Надано рекомендації для захисту об'єктів критичної інфраструктури від дії безпілотних літальних апаратів різної класифікації, а саме: застосування комплексів радіоелектронної боротьби, систем радіолокації, тепловізійних систем, систем звукового виявлення безпілотних літальних апаратів і використання для їх знешкодження крупнокаліберних гарматних-кулеметних стаціонарних і пересувних зенітних комплексів, переносних і стаціонарних ракетних систем протиповітряної оборони та систем перехоплення безпілотних літальних апаратів за допомогою спрямованого електромагнітного сигналу.*

Ключові слова: *об'єкт критичної інфраструктури, безпілотні літальні апарати, національна безпека.*

ПОСТАНОВКА ПРОБЛЕМИ

Україна як держава, яка зараз перебуває в стані повномасштабної війни, постійно розв'язує одну з найголовніших проблем виживання держави, — збереження від знищення об'єктів критично інфраструктури. До їх складу належать об'єкти ядерно-паливного циклу, теплові, гідроелектричні, вітрові та сонячні станції генерації енергії, інші підприємства, які є стратегічними об'єктами.

Ворог активно використовує безпілотні літальні апарати (БПЛА) для атаки об'єктів критичної інфраструктури України. З огляду на те, що безпілотні літальні апарати мають дуже низьку собівартість у порівнянні зі звичайними пілотованими літальними апаратами, не потребують довготривалого навчання льотного персоналу і можуть вироблятись у великих кількостях, то можна прогнозувати зростання числа їх використання та збільшення варіантів застосування проти об'єктів критичної інфраструктури України.

Метою статті є опис типових безпілотних літальних апаратів, варіанти їх застосування та методи і засоби захисту об'єктів критичної інфраструктури.

ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ

Опис типового об'єкта критичної інфраструктури

Об'єкти критичної інфраструктури — підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, а також призвести до значних матеріальних і фінансових збитків, людських жертв [1].

До таких об'єктів можна зарахувати:

1) об'єкти атомної енергетики (АЕС, сховища ядерного палива та радіоактивних відходів);

2) гідроелектричні станції та інші гідротехнічні споруди;

3) морські порти та термінали;

4) спорудження зв'язку (радіо та телевізійні вежі, наземні та підземні пункти комунікаційних вузлових з'єднань, антенні поля та телефонні станції);

5) теплові електростанції та котельні;

6) лінії електропередач і трансформаторні розподільчі станції;

7) об'єкти авіаційної та космічної інфраструктури;

8) об'єкти інфраструктури залізничного та автомобільного транспорту (тунелі, шляхопроводи, розв'язки), а також канатні дороги;

9) метрополітен;

10) небезпечні виробництва (підприємства).

Як приклад об'єкта критичної інфраструктури розглянемо атомну електростанцію.

Атомна електростанція (АЕС) — електростанція, у якій атомна (ядерна) енергія перетворюється на електричну. Генератором енергії на АЕС є атомний реактор. Тепло, що виділяється в реакторі внаслідок ланцюгової реакції поділу ядер деяких важких елементів, потім так само як і на звичайних теплових електростанціях (ТЕС), перетвориться на електроенергію. На відміну від теплоелектростанцій, що працюють на органічному паливі, АЕС працює на ядерному паливі (переважно ^{232}U, ^{235}U, ^{239}Pu) [2]. Принципову схему розташування основних об'єктів АЕС показано на **рис. 1**.

Також на території, де розташовуються основні об'єкти АЕС, також можуть знаходиться сховища відпрацьованого ядерного палива та інші допоміжні споруди. Обов'язково біля АЕС розташовується ставок-охолоджувач, без якого нормальне функціонування атомної станції неможливе.

Територія, де розміщено основні та допоміжні споруди АЕС і ставок охолоджувач, знаходиться під воєнізованою охороною та оточена системою фізичного захисту, що представлено багатобар'єрним комплексом із системами візуального та електронного спостереження за об'єктами, які представляють потенційну небезпеку для стійкого функціонування об'єкта критичної інфраструктури.

З наведеного вище випливає, що ми маємо порівняно велику територію з декількома десятками будівель різної формації, яка потребує захисту від різних типів БПЛА, що можуть використовуватися зловмисниками.

Типізація БПЛА

Розглянемо компоненти безпілотних авіаційних систем. Базова установка невеликого безпілотного літального апарату складається з пульта дистанційного керування, за допомогою

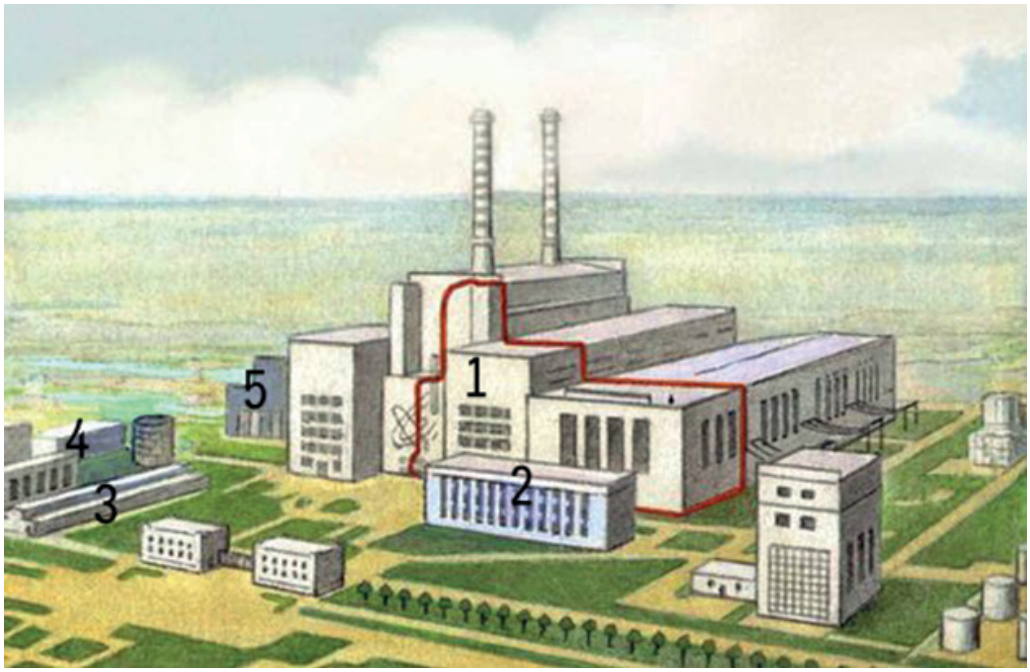

Рис. 1. Принципова схема розташування основних об'єктів АЕС

Примітка: 1 — головний корпус (розміщено ядерний реактор); 2 — службовий корпус; 3 — корпус хімводоочищення; 4 — газгольдерна; 5 — корпус спецводоочищення.

якого оператор по каналу електромагнітного зв'язку керує безпілотним літальним апаратом. Більші системи можуть також включати спеціальну наземну станцію управління для запуску та керування польотом для проведення операції. Ще більші системи зазвичай використовують космічний зв'язок для каналів передачі даних і складаються з такої інфраструктури, як вантажівки, контейнери або будівлі, у яких зазвичай розміщується комп'ютерне обладнання та програмне забезпечення, що є необхідними для роботи всієї системи [3].

Останніми десятиліттями безпілотні авіаційні системи використовувалися в усіх видах військової служби: від портативних мікро-БПЛА до тактичних систем середнього розміру та повноцінних дистанційно пілотованих літальних апаратів. Водночас на цивільному ринку спостерігається експоненційне зростання переважно невеликих систем, що призначені для суспільного та розважального використання. Однак останній варіант використання привернув увагу правоохоронних органів і служб, які займаються фізичним захистом об'єктів критичної інфраструктури, через можливе застосування готових комерційних дронів поблизу і над цими об'єктами [4].

Здійснимо класифікацію та категоризацію БПЛА з позицій, які важливі при використанні їх проти об'єктів критичної інфраструктури.

По-перше, усі БПЛА поділяють на дві великі групи незалежно від їхніх розмірів, формфакторів і типів рушіїв, це безпілотні літальні апарати, які керуються оператором, або ті, що виконують свій політ за заздалегідь запрограмованим маршрутом польоту [5–7].

Керовані БПЛА, як і ті, що прямують за заздалегідь запрограмованим маршрутом, можуть виконувати як розвідувальні, так і атакувальні завдання. Якщо некеровані БПЛА можуть використовуватися для розвідки заздалегідь запланованої території, або здійснювати атаку стаціонарного, заздалегідь розвіданого об'єкта критичної інфраструктури, то керовані БПЛА більш гнучкі в цьому контексті. Вони можуть використовуватися як "дрони-камікадзе" по стаціонарних цілях, так і по цілях, які переміщуються, а також бути носієм озброєння для атаки на наземні об'єкти критичної інфраструктури. Окрім того, вони можуть оперативно виконувати розвідку в швидкій зміні оперативної обстановки і здійснювати підтримку диверсійних груп при здійсненні вторгнення на об'єкт критичної інфраструктури.

Наступний важливий критерій класифікації БПЛА в інтересах захисту об'єктів критичної інфраструктури — це розміри самих БПЛА.

З критерію розміру випливають такі важливі супутні параметри, як корисне навантаження, яке можуть нести БПЛА, і відповідно робоча висота застосування БПЛА при його застосуванні проти об'єкта критичної інфраструктури.

У структурі Північноатлантичного альянсу БПЛА розділяють на три спеціалізовані класи:

- клас I — мікро-, міні- та малі БПЛА;
- клас II — тактичні системи середнього розміру;
- клас III — середньовисотні та дальні БПЛА.

Розглянувши лише вищенаведені три різні класи, а також розмір, робочу висоту, корисне навантаження, можливість здійснення керування, можна дійти висновку, що протидія цьому БПЛА вимагає безлічі різних підходів, специфічних для кожного класу.

Імовірні сценарії використання БПЛА проти об'єктів критичної інфраструктури

Розглянемо ймовірні сценарії використання різних типів БПЛА проти об'єкта критичної інфраструктури.

Перший сценарій застосування БПЛА проти об'єктів критичної інфраструктури — це розвідка. Припустимо, що група зловмисників планує диверсійні акції на об'єкті критичної інфраструктури, а саме — на об'єкті АЕС. Для здійснення запланованого, зловмисники мають зібрати якнайбільше інформації про: стан фізичного захисту об'єкта; кількість персоналу, який залучений до забезпечення безпеки; технічні системи забезпечення захисту об'єкта [8].

Згідно з класифікацією Північноатлантичного альянсу, БПЛА розрізняють за розміром і робочою висотою.

Клас I — мікро-, міні- та малі БПЛА.

Такі безпілотні літальні апарати можуть використовуватись тоді, коли оператор БПЛА знаходиться на відстані від декількох десятків кілометрів до декількох десятків метрів від зовнішнього периметра фізичного захисту об'єкта критичної інфраструктури, а висота застосування не перевищує півтори, дві тисячі метрів [9].

Застосування таких БПЛА полягає в тому, що зловмисники залишаються непоміченими чи неідентифікованими, адже можуть влаштуватися на відстані не більше декількох кілометрів від об'єкта атомної енергетики, наприклад, вийняли квартиру в місті-супутнику чи прилеглих до об'єкта критичної інфраструктури населених пунктах і проводити скритне рекогностування місцевості біля об'єкта або сам об'єкт критичної інфраструктури.

Мікро-БПЛА зловмисники можуть випускати для розвідувальних завдань з автотранспорту,

видаючи себе за рибалок, грибників або туристів.

Головна небезпека БПЛА першого класу — це їхні малі розміри, що призводить до їх важкої фіксації персоналом і системами фізичного захисту. Якщо використовувати такі безпілотні літальні системи вночі, то їх виявлення вкрай ускладнено або взагалі неможливо.

Також малі розміри цих БПЛА дозволяють проникати вглиб території, що охороняється, непоміченими і непомітно виявляти та знімати інформацію безпосередньо біля кожної будівлі чи функціонального вузла об'єкта критичної інфраструктури [10–12].

Головний недолік цих систем, переважно невеликий час роботи, що вимагає від зловмисників більшої повторюваності їх застосування, що може призвести як до виявлення і знешкодження БПЛА, так і самої диверсійної групи.

Клас II — тактичні системи середнього розміру.

Такі системи можуть діяти на відстані від декількох десятків до декількох сотень кілометрів від зовнішнього периметра фізичного захисту об'єкта критичної інфраструктури, а висота їх використання сягає декількох тисяч метрів.

Застосування таких БПЛА полягає в тому, що зловмисникам не потрібно наближатися безпосередньо до периметра об'єкта критичної інфраструктури, а можна влаштуватися за сотню кілометрів від об'єкта і вести спостереження.

Такі БПЛА можуть довго знаходитися в повітрі, багато годин, і з відносно великої висоти спостерігати за ядерним об'єктом і передавати інформацію зловмисникам. Через те, що час польоту цих БПЛА досить великий, то зловмисники можуть отримувати інформацію про довготривалі процеси, що відбуваються на об'єкті критичної інфраструктури лише за один виліт БПЛА такого типу.

Основний недолік цих систем випливає з їхніх розмірів. Вдень їх можна візуально побачити неозброєним оком, або ж за допомогою оптичних приладів спостереження, а в ночі — за допомогою систем радіолокації малої та середньої дальності або інфрачервоних оптичних приладів.

Клас III — середньовисотні та дальні БПЛА.

Ці БПЛА мають дуже великий радіус дії і час перебування в повітрі, що обчислюється тисячами кілометрів і десятками годин, а висота застосування може досягати десятки кілометрів.

Такий БПЛА буде застосовуватись як довготривалий засіб спостереження за об'єктом критичної інфраструктури. Він може діяти як в інтересах координації диверсійної групи, так і декількох диверсійних груп. Також такі БПЛА діють на дуже великій висоті та можуть вести спостереження і координації на великих відстанях за багато десятків кілометрів від об'єкта критичної інфраструктури.

Візуально та за допомогою оптичних приладів спостерігати такі безпілотні апарати практично неможливо. Їх можна детектувати лише за допомогою радіолокаційних засобів середньої і великої дальності.

Другий сценарій застосування безпілотних літальних апаратів проти об'єктів критичної інфраструктури — це безпосередньо атака. Здійснення зловмисниками заходів на повне знищення об'єкта або виведення з ладу основних технологічних вузлів.

Клас I — мікро-, міні- та малі БПЛА.

Цей клас БПЛА передбачає використання їх при безпосередньому озброєному зіткненні терористичної бойової групи з силами фізичного захисту об'єкта критичної інфраструктури.

Мікро- і міні БПЛА будуть використовуватися диверсійною групою як розвідники вогневих позицій сил захисту безпосередньо на полі бою. Малі БПЛА можуть використовуватись як для дорозвідки бойової обстановки на полі бою. Також БПЛА можуть нести вибухові прилади, наприклад, гранати, невеликі міни для ураження живої сили чи кумулятивні заряди для ураження легкоброньованих цілей, окопів, бліндажів сил фізичного захисту ядерного об'єкта.

Клас II — тактичні системи середнього розміру.

Для подальшого аналізу застосування цього класу БПЛА треба розділити їх на керовані оператором, та ті, що виконують політ в автоматичному режимі.

Диверсійні групи можуть використовувати БПЛА, які виконують політ в автоматичному режимі, як ударні дрони-камікадзе. Один зі сценаріїв їх застосування — це запуск таких дронів за певним маршрутом, які містять вибухові речовини. За деякий час до вторгнення диверсійних груп до об'єкта критичної інфраструктури такі БПЛА проводять атаку на об'єкт, що може спричинити пожежі, руйнування, загибель або травмування людей, паніку серед персоналу. Такий попередній удар, полегшує виконання завдання для диверсійної групи.

БПЛА, які керуються оператором, можуть нести керовані або некеровані ракети, вибухівку та інше озброєння. Такі БПЛА можуть завдавати удару по укріплених пунктах оборони і критичним вузлам фізичного захисту об'єкта критичної інфраструктури [13–15].

Клас III — середньовисотні та дальні БПЛА.

Такий тип БПЛА може нести на собі важке озброєння типу ракет класу "повітря-поверхня",

які можуть вражати важко укріплені вузли фізичного захисту і оборони, засоби протиповітряної оборони.

Такі БПЛА піднімаються в повітря заздалегідь і підлітають до об'єкта критичної інфраструктури, щоб підтримати вогневими засобами ураження диверсійні групи чи завдати превентивного удару по системах радіолокаційного захисту, системам радіоелектронної боротьби та вузлам зв'язку [16].

Також після використання засобів ураження, за рахунок тривалого періоду знаходження в повітрі, за допомогою таких безпілотних апаратів, зловмисники можуть проводити корегування дій своїх диверсійних груп або групи в реальному масштабі часу.

Методи та засоби захисту об'єктів критичної інфраструктури від загроз із боку БПЛА

Варто зазначити, що перед тим, як ми розглянемо методи та засоби протидії БПЛА, варто звернути увагу на використання окремих оперативно-розшукових заходів у зоні відповідальності органів, що забезпечують фізичний захист об'єктів критичної інфраструктури.

Застосування БПЛА досить сильно знижує їхню ефективність, коли біля об'єкта, що охороняється, відсутні, як мінімум коригувальники атаки, а як максимум — диверсійно-розвідувальні групи, в інтересах яких працюють вищенаведені безпілотні літальні апарати.

Тому ефективна робота органів внутрішнього правопорядку, а також контррозвідки є запорукою безпечного функціонування об'єкта критичної інфраструктури.

Протидію БПЛА різних класів будемо вибудовувати за принципом ешелонованого захисту.

За перший рубіж оборони приймемо рубіж протидії середньовисотним та дальні БПЛА.

Виходячи з вищенаведених характеристик цього класу БПЛА та їхніх ударних і розвідувальних можливостей, перший рубіж оборони об'єкта ядерної енергетики має охоплювати радіолокаційні системи великої дальності, а також системи перехоплення, які основані на ракетному озброєні.

Також для перехоплення БПЛА такого класу можна і необхідно застосовувати винищувачі військ протиповітряної оборони.

Другий рубіж оборони — це рубіж протидії тактичним системам БПЛА середнього розміру.

Протидія таким БПЛА може здійснюватися системами з зенітно-артилерійським і ракетним озброєнням середнього радіуса дії та переносними зенітно-ракетними комплексами. Також можна використовувати переносні та пересувні кулемети великого калібру.

Для виявлення таких типів БПЛА доцільно використовувати акустичні та інфрачервоні методи виявлення.

Проти керованих БПЛА доцільно застосовувати системи радіоелектронної боротьби для встановлення радіоелектронних перешкод.

Третій рубіж оборони — це так званий останній рубіж оборони, а саме — протидія мікро-, міні- та малим БПЛА.

Протидіяти такому класу БПЛА дуже важко, з огляду на їхню швидкість і малорозмірність. Якщо такі БПЛА працюють вночі або в умовах обмеженої видимості, то завдання щодо знаходження й ураження таких БПЛА стає майже неможливим.

Стрілецька та крупнокаліберна зброя різних калібрів, переносні зенітні комплекси та різноманітні системи протиповітряної оборони ближнього радіуса дії показують дуже малу ефективність, враховуючи що такі БПЛА можуть із дуже великою швидкістю змінювати напрямок свого руху, та за геометричними параметрами дуже складно визначається та ідентифікується.

Тому дуже ефективною зброєю та системами захисту будуть різноманітні комплекси радіоелектронної боротьби. Встановлення потужних радіоелектронних перешкод позбавляє операторів БПЛА зворотного зв'язку і нівелює їх використання.

Також при візуальному виявленні БПЛА можуть бути використані переносні електромагнітні системи перехоплення БПЛА, а також власні БПЛА з системами протидії або захоплення ворожих БПЛА [17].

ВИСНОВКИ

1. Безпілотні літальні апарати поділяють на дві великі групи незалежно від їхніх розмірів, формфакторів і типів рушіїв. Це безпілотні літальні апарати, які керуються оператором, або ті, що виконують свій політ за заздалегідь запрограмованим маршрутом польоту. Також є три спеціалізовані класи цих апаратів відповідно до класифікації Північноатлантичного альянсу.

2. Безпілотні літальні апарати можуть використовуватися проти об'єктів критичної інфраструктури за такими головними типовими сценаріями, як: розвідка на користь зловмисників проти об'єкта атомної енергетики; безпосередня атака на об'єкт критичної інфраструктури за допомогою засобів ураження, які знаходяться на борту; підтримка дій диверсійних груп при безпосередній атаці на об'єкт.

3. Гарантування безпеки об'єкта ядерної енергетики будується за принципом ешелонованого захисту. Перший рубіж оборони — це протидія середньовисотним і дальнім

безпілотним літальним апаратам класу III, другий рубіж оборони — це протидія тактичним системам середнього розміру БПЛА класу II, третій — "останній рубіж оборони", що передбачає протидію мікро-, міні- і малим безпілотним літальним апаратам класу I.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про критичну інфраструктуру [Електронний ресурс] : Закон України від 16 листопада 2021 р. № 1882-IX. — Режим доступу: https://zakon.rada.gov.ua/laws/show/en/1882-20?lang=uk#Text.
2. *Martin W.* Nuclear power [Electronic resource] / W. Martin // Encyclopedia Britannica. — 2024, March 14. — Access mode: https://www.britannica.com/technology/nuclear-power.
3. *Khalife J.* On the achievability of submeter-accurate UAV navigation with cellular signals exploiting loose network synchronization / J. Khalife, Z. M. Kassas // IEEE Transactions on Aerospace and Electronic Systems. — 2022. — Vol. 58. — Issue 5. — P. 4261–4278. DOI: http://doi.org/10.1109/TAES.2022.3162770.
4. *Liu W.* A hybrid optimization framework for UAV reconnaissance mission planning / W. Liu, T. Zhang, S. Huang, K. Li // Computers & Industrial Engineering. — 2022. — Vol. 173. — 108653. DOI: http://dx.doi.org/10.1016/j.cie.2022.108653.
5. A review of artificial intelligence applied to path planning in UAV swarms / A. Puente-Castro, D. Rivero, A. Pazos, E. Fernandez-Blanco // Neural Comput & Applic. — 2022. — Vol. 34. — P. 153–170. DOI: http://dx.doi.org/10.1007/s00521-021-06569-4.
6. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends / Syed Agha Hassnain Mohsan, Nawaf Qasem Hamood Othman, Yanlong Li, Mohammed H. Alsharif, Muhammad Asghar Khan // Intell Serv Robotics. — Vol. 16. — P. 109–137. DOI: http://dx.doi.org/10.1007/s11370-022-00452-4.
7. *Ganti S. R.* Design of low-cost on-board auto-tracking antenna for small UAS / S. R. Ganti, Y. Kim // In Proceedings of the 12th International Conference on Information Technology-New Generations, Las Vegas, NV, USA (13–15 April 2015). — 2015. — P. 273–279.
8. Countering rogue drones / FICCI Committee on Drones. — EY, 2018. — 32 p.
9. A Design Methodology for Controlling, Monitoring and Allocating Unmanned Vehicles / E. de Visser, M. S. Cohen, M. LeGoullon, O. Sert, A. Freedy, E. Freedy, G. Weltman, R. Parasuraman // Third International Conference on Human Centered Processes (HCP-2008). — 2008. — 5 p.
10. *Kratky M.* The non-destructive methods of fight against UAVs / M. Kratky, V. Minarik // International Conference on Military Technologies (ICMT). – IEEE, 2017. — P. 690–694.
11. Real-time counter-UAV system for long distance small drones using double pan-tilt scan laser radar / Byeong Hak Kim, Danish Khan, Wonju Choi, Min Young Kim // Preceding SPIE. — 2019. — Vol. 11005, Laser Radar Technology and Applications XXIV, 110050C (2 May 2019). DOI: http://doi.org/10.1117/12.2520110.
12. Capture of UAVs Through GPS Spoofing / J. Gaspar, R. Ferreira, P. Sebastião, N. Souto // 2018 Global Wireless Summit (GWS). — IEEE, 2018. — P. 21–26.
13. *Müller W.* Open architecture of a counter UAV System / W. Müller, F. Reinert, D. Pallmer // Preceding SPIE. — 2018. — Vol. 10651, Open Architecture. Open Business Model Net-Centric Systems and Defense Transformation. 1065106. DOI: http://doi.org/10.1117/12.2305606.
14. *Hartmann K.* UAV exploitation: A new domain for cyber power / K. Hartmann, K. Giles // 8th International Conference on Cyber Conflict (CyCon) IEEE. — 2016. — P. 205–221.
15. *Michalski D.* Protection against drone activity [Electronic resource] / Daniel Michalski, Anna Michalska // Security Forum. — 2017. — Vol. 1. — No. 1. — P. 73–83. — Access mode: https://wsb.edu.pl/files/pages/634/security_forum_01_2017_8druk.pdf.
16. Directed Energy Weapons: DOD should focuse on Transition Planning : Report to Congressional Committees [Electronic resource] // US GAO. — 2023. — 45 p. — Access mode: https://www.gao.gov/assets/gao-23-105868.pdf.
17. *Vashisht P.* Modern Counter Drone Systems — A Technology Review [Electronic resource] / P. Vashisht. — Apr. 2021. — 4 p. — Access mode: https://www.mistralsolutions.com/wp-content/uploads/2021/07/Modern-Counter-Drone-Systems.pdf.

REFERENCES

1. Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16 lystopada 2021 r. № 1882-IX [About critical infrastructure. Law of Ukraine on November 16, 2021 No. 1882-IX]. Retrieved from: https://zakon.rada.gov.ua/laws/show/en/1882-20?lang=uk#Text [in Ukr.].
2. Martin, W. (2024). Nuclear power. *Encyclopedia Britannica.* Retrieved from: https://www.britannica.com/technology/nuclear-power.
3. Khalife, J., & Kassas, Z. M. (2022). On the achievability of submeter-accurate UAV navigation with cellular signals exploiting loose network synchronization. *IEEE Trans. Aerosp. Electron. Syst. 58,* 4261–4278. DOI: http://doi.org/10.1109/TAES.2022.3162770.
4. Liu, W., Zhang, T., Huang, S., & Li, K. (2022). A hybrid optimization framework for UAV reconnaissance mission planning. *Comput. Ind. Eng.* 173, 108653. DOI: http://dx.doi.org/10.1016/j.cie.2022.108653.
5. Puente-Castro, A., Rivero, D., & Pazos, A. (2022). Fernandez-Blanco, E. A review of artificial intelligence applied to path planning in UAV swarms. *Neural Comput & Applic. 34*, 153–170. DOI: http://dx.doi.org/10.1007/s00521-021-06569-4.
6. Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot. 16,* 109–137. DOI: http://dx.doi.org/10.1007/s11370-022-00452-4.
7. Ganti, S. R., & Kim, Y. (2015). Design of low-cost on-board auto-tracking antenna for small UAS. *In Proceedings of the 12th International Conference on Information Technology-New Generations*, Las Vegas, NV, USA. P. 273–279.
8. Countering rogue drones. (2018). *FICCI Committee on Drones, EY.* 32 p.
9. de Visser, E., Cohen, M. S., LeGoullon, M., Sert, O., Freedy, A., Freedy, E., Weltman, G., & Parasuraman, R. (2008). A Design Methodology for Controlling, Monitoring and Allocating Unmanned Vehicles. *Third International Conference on Human Centered Processes (HCP-2008).* P. 1–5.
10. Kratky, M., & Minarik, V. (2017). The non-destructive methods of fight against UAVs. *International Conference on Military Technologies (ICMT). IEEE.* P. 690–694.

11. Kim, B. H., Khan, D., Choi, W., & Kim, M. Y. Real-time counter-UAV system for long distance small drones using double pan-tilt scan laser radar. Preceding SPIE11005, *Laser Radar Technology and Applications XXIV*, 110050C (2 May 2019). DOI: http://doi.org/10.1117/12.2520110.
12. Gaspar, J., Ferreira, R., Sebastião, P., & Souto, N. (2018). Capture of UAVs Through GPS Spoofing. *2018 Global Wireless Summit (GWS).* IEEE. P. 21–26.
13. Müller, W., Reinert, F., & Pallmer, D. (2018). Open architecture of a counter UAV System. *Preceding SPIE 10651, Open Architecture. Open Business Model Net-Centric Systems and Defense Transformation*. 1065106. DOI: http://doi.org/10.1117/12.2305606.
14. Hartmann, K., & Giles, K. (2016). UAV exploitation: A new domain for cyber power. *8th International Conference on Cyber Conflict (CyCon). IEEE*. P. 205–221.
15. Michalski, D., & Michalska, A. (2017). Protection against drone activity. *Security Forum. 1* (1), 73–83. Retrieved from: https://wsb.edu.pl/files/pages/634/security_forum_01_2017_8druk.pdf.
16. US GAO (2023). Report to Congressional Committees. Directed Energy Weapons: DOD should focuse on Transition Planning. Retrieved from: https://www.gao.gov/assets/gao-23-105868.pdf.
17. Vashisht, P. (2021). Modern Counter Drone Systems — A Technology Review. Retrieved from: https://www.mistralsolutions.com/wp-content/uploads/2021/07/Modern-Counter-Drone-Systems.pdf.

M. M. DIVIZINIUK, D. Sc. in Physics and Mathematics
O. V. FARRAKHOV, PhD in Engineering
L. A. MARTSEVA, D. Sc. in Pedagogy
A. O. KOTSIUBYNSKYI, PhD in Physics and Mathematics
O. V. VLASENKO, Senior Lecturer

ANALYSIS OF SCENARIOS OF THE USE OF UNMANNED AIRCRAFT AGAINST CRITICAL INFRASTRUCTURE OBJECTS

Abstract. *The purpose of the work is to analyze the use of unmanned aerial vehicles in ensuring the safety of critical infrastructure facilities. To achieve the goal, the following tasks were solved. First, the problem was considered and the research task was set. It is shown that unmanned aerial vehicles pose a significant danger to critical state infrastructure facilities. At the next stage, typical objects of the state's critical infrastructure are described and a typical nuclear power plant is taken as an example. It is shown that unmanned aerial vehicles have a wide range of typification both by design features and by classification features. The analysis was carried out and possible ways of using unmanned aerial vehicles against the object of critical infrastructure were presented. It is shown that small and medium-sized unmanned aerial vehicles can be used by criminals as both reconnaissance and local strike means of damaging the infrastructure of a critical infrastructure object. Large unmanned aerial vehicles can be used as unguided means of destruction and as means of supporting the actions of sabotage groups. Recommendations are provided for the protection of critical infrastructure objects from the action of unmanned aerial vehicles of various classifications, namely the use of electronic warfare systems, radar systems, thermal imaging systems, sound detection systems of unmanned aerial vehicles and the use of large-caliber cannon-machine gun stationary and mobile anti-aircraft systems for their neutralization , portable and stationary anti-aircraft missile systems and systems for interception of unmanned aerial vehicles using a directed electromagnetic signal.*

Keywords: *critical infrastructure facility, unmanned aerial vehicles, national security.*

ІНФОРМАЦІЯ ПРО АВТОРІВ

Дівізінюк Михайло Михайлович — д-р фіз.-мат. наук, проф., голов. н. с., Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, просп. ак. Палладіна, 34А, м. Київ, Україна, 03142; divizinyuk@ukr.net; ORCID: 0000-0002-5657-2302

Фаррахов Олександр Володимирович — канд. техн. наук, пров. н. с., Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, просп. ак. Палладіна, 34А, м. Київ, Україна, 03142; farrakhov@ukr.net; ORCID: 0000-0003-4988-126X

Марцева Людмила Андріївна — д-р пед. наук, доц., Державний університет "Житомирська політехніка", вул. Чуднівська, 103, м. Житомир, Україна, 10005; l.a.martseva@gmail.com; ORCID: 0000-0001-5037-6565

Коцюбинський Андрій Олегович — канд. фіз.-мат. наук, доц., Івано-Франківський національний технічний університет нафти і газу, вул. Карпатська, 15, м. Івано-Франківськ, Україна, 76019; Radijrlife@gmail.com; ORCID: 0000-0003-1135-3568

Власенко Олег Васильович — ст. викладач кафедри інженерії програмного забезпечення, Державний університет "Житомирська політехніка", вул. Чуднівська, 103, м. Житомир, Україна, 10005; oleh.vls@gmail.com; ORCID: 0000-0001-6697-2150

INFORMATION ABOUT THE AUTHORS

Diviziniuk M. M. — D. Sc. in Physics and Mathematics, Professor, Chief Research Associate, Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, 34A, Academician Palladin Ave, Kyiv, Ukraine, 03142; divizinyuk@ukr.net; ORCID: 0000-0002-5657-2302

Farrakhov O. V. — PhD in Engineering, Leading Researcher, Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, 34A, Academician Palladin Ave, Kyiv, Ukraine, 03142; farrakhov@ukr.net; ORCID: 0000-0003-4988-126X

Martseva L. A. — D. Sc. in Pedagogy, assistant professor, Zhytomyr Polytechnic State University, 103, Chudnivsyka Str., Zhytomyr, Ukraine, 10005; l.a.martseva@gmail.com; ORCID: 0000-0001-5037-6565

Kotsiubynskyi A. O. — PhD in Physics and Mathematics, Assistant Professor, Ivano-Frankivsk National Technical University of Oil and Gas, 15, Karpatska Str., Ivano-Frankivsk, Ukraine, 76019; Radijrlife@gmail.com; ORCID: 0000-0003-1135-3568

Vlasenko O. V. — Senior Lecturer at the Department of Software Engineering, Zhytomyr Polytechnic State University, 103, Chudnivsyka Str., Zhytomyr, Ukraine, 10005; oleh.vls@gmail.com; ORCID: 0000-0001-6697-2150

http://doi.org/10.35668/2520-6524-2024-3-13
УДК 004.054:[004.032.26+004.85]

Я. О. ІСАЄНКОВ, аспірант
О. Б. МОКІН, д-р техн. наук, проф.

МЕТОД ОЦІНКИ ЧАСТКОВО ЗГЕНЕРОВАНИХ ДАНИХ

Резюме. *Останніми роками генеративні моделі, зокрема автокодувальники, генеративні змагальні мережі та дифузійні моделі, стали невіддільною частиною інновацій у різних галузях, таких, як мистецтво, дизайн, медицина тощо. Завдяки здатності створювати нові зразки даних, вони відкривають широкі можливості для автоматизації та вдосконалення процесів. Однак оцінка якості згенерованих даних залишається складним завданням, оскільки традиційні методи не завжди адекватно відображають різноманітність і реалістичність створених зразків. Зокрема це стосується часткового генерування даних, де зміни застосовуються лише до окремих частин зображення, що значно ускладнює оцінку їх якості.*

У цій статті розглянуто різні підходи до оцінки генеративних моделей, зокрема такі автоматичні метрики, як Inception Score і Fréchet Inception Distance, влучність, повнота, щільність і покриття, а також метод із залученням людини HYPE. Хоча ці метрики добре зарекомендували себе в оцінюванні результатів традиційного генерування, їх використання у випадку частково згенерованих даних може бути недоцільним через їх обмеження. Для розв'язання цієї проблеми в статті запропоновано новий метод оцінювання частково згенерованих даних із залученням людини. Цей метод базується на аналізі трансформованих зображень користувачами, які визначають зони, що зазнали змін, і оцінює їхню якість за допомогою метрик влучності, повноти, F1-міри, шукаючи перетини між реальними зонами та вибраними користувачем із використанням IoU. Запропонований підхід забезпечує більш об'єктивну оцінку реалістичності та якості згенерованих фрагментів зображень під час трансформацій.

Наведено практичний приклад застосування розробленого методу на наборі даних панорамних стоматологічних знімків, де оцінювалася якість трьох моделей: 1) ГЗМ на основі U-генератора; 2) та сама модель, але з післяобробкою вихідного зображення і сегментаційної маски; 3) самовалідована ГЗМ. Оцінку проводили 30 осіб. Середні значення F1-міри для цих моделей становили 0,78, 0,27 і 0,20 відповідно. Оскільки нижчі значення F1-міри в цьому випадку свідчать про кращі результати (чим точніше користувачі ідентифікували трансформації, тим гірше працювала модель), найкращою моделлю за цією метрикою є самовалідована ГЗМ, що також підтверджується суб'єктивними оцінками, зазначеними в працях авторів.

Ключові слова: *аугментація, генерування даних, генеративна змагальна мережа, ГЗМ, комп'ютерний зір, глибоке навчання, самовалідована ГЗМ, оцінювання, нейронні мережі.*

ВСТУП

Генеративні мережі, зокрема автокодувальники [1], генеративні змагальні мережі (ГЗМ) [2], дифузійні моделі [3] стали потужним інструментом для створення таких нових зразків даних, як зображення, текст або навіть музика. Їх широке застосування охоплює різні галузі, включаючи мистецтво, дизайн, медицину.