дій. Також варто зазначити, що мобільність і автономність стають пріоритетними характеристиками сучасної техніки. Відповідно, зростає потреба у спеціалізованій підготовці особового складу для експлуатації таких систем. Додатково актуальним є розвиток національних виробничих потужностей, які здатні оперативно адаптувати техніку до умов конкретного театру бойових дій.

Однією з найбільш визначальних змін є трансформація поля бою на користь мережево-центричних операцій, де головну роль відіграє швидке отримання, обробка й передача інформації. Завдяки БПЛА та супутниковому зв'язку (наприклад, Starlink) українські підрозділи отримали можливість ефективно координувати свої дії та вражати ворога на великих відстанях. Закон України «Про національну безпеку України» (ст. 1) визначає технологічне оновлення та інтеграцію новітніх засобів оборони як пріоритет національної політики. У цих умовах модернізація технічного оснащення має стати системним процесом, що включає як закупівлю сучасного озброєння, так і розвиток інфраструктури для його обслуговування та підготовки персоналу.

Застосування дронів-камікадзе типу FPV значно підвищило ефективність боротьби з бронетехнікою противника, дозволяючи вражати її у слабко захищених місцях. Водночас мобільні групи з ПТРК, які мають цифрову підтримку, можуть діяти автономно в умовах інформаційного контролю. В практиці підрозділів також активно використовуються планшети з нанесенням цифрових карт, засоби нічного бачення, цифрові далекоміри, що виводять бойові можливості бійців на новий рівень. Яскравим прикладом інтеграції новітніх засобів є використання артилерійських систем типу М777 у поєднанні з дронами-коригувальниками. Це забезпечує надзвичайно точне вогневе ураження при мінімальних витратах ресурсів. Ще одним прикладом є створення ударних дронових рот, які використовуються для ураження тилових об'єктів ворога на глибину до 40 км.

Висновок: застосування сучасного озброєння та техніки радикально змінює підходи до ведення бойових дій і вимагає нових форм підготовки особового складу. Український досвід демонструє, що технічна перевага може компенсувати чисельну перевагу ворога. Отримані результати мають як теоретичну, так і практичну цінність, адже формують підґрунтя для створення нових бойових доктрин. На їх основі можливе подальше вдосконалення системи управління військами та технічного забезпечення сектору безпеки й оборони України.

Суслов Роман,
викладач кафедри тактики та
тактико-спеціальної підготовки,
Київський інститут Національної гвардії України

АВТОМАТИЧНИЙ ЗАХИСТ ДЕРЖАВНИХ БУДІВЕЛЬ ВІД БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ (БПЛА) РІЗНИХ ТИПІВ ЗА ДОПОМОГОЮ СИСТЕМИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ (РЕБ) З АВТОМАТИЧНИМ ВИЯВЛЕННЯМ ЧАСТОТ УПРАВЛІННЯ ТА ЇХ ПОДАВЛЕННЯМ

Актуальність цієї теми зумовлена тим, що сьогодні БПЛА стали доступним і потужним інструментом, який, на жаль, може використовуватися не лише в цивільних цілях, а й для здійснення терористичних актів, шпигунства, доставки заборонених речовин, а також атак на критичну інфраструктуру та державні будівлі. Різноманітність типів БПЛА, від малих комерційних дронів до більш складних військових апаратів, створює складне завдання для існуючих систем безпеки. Захист державних будівель є критично важливим для забезпечення національної безпеки, збереження життя людей та запобігання матеріальним збиткам. При цьому традиційні методи охорони часто виявляються недостатньо ефективними проти сучасних БПЛА, оскільки ті можуть діяти на низьких висотах, мати невеликі розміри та використовувати різноманітні канали зв'язку.

Концепція пропонованої автоматизованої системи захисту полягає у створенні багаторівневої інтегрованої системи, здатної в автоматичному режимі виявляти, ідентифікувати, класифікувати та нейтралізувати БПЛА, що наближаються до захищеної зони. Ключовим елементом такої системи є комплекс РЕБ, що здійснює автоматичне сканування та аналіз радіочастотного спектра.

До основних компонентів системи належать кілька підсистем. Система виявлення включає малогабаритні радіолокаційні станції (РЛС) невеликого радіусу дії для дальнього виявлення об'єктів у повітрі, визначення їхніх координат, швидкості та траєкторії руху, причому РЛС можуть бути оптимізовані для виявлення малорозмірних та низьколітаючих цілей. Для прикладу малогабаритна оглядова РЛС "Снов". Також використовуються оптико-електронні системи (ОЕС), що містять тепловізори та камери високої роздільної здатності для візуального підтвердження цілі, її ідентифікації за формою, розмірами, наявністю підвісів та для її супроводження. Додатково застосовуються акустичні датчики для виявлення характерного звуку двигунів БПЛА, особливо на малих відстанях, та радіочастотні сканери, які постійно моніторять радіоефір у широкому діапазоні частот з метою виявлення сигналів управління та телеметрії БПЛА.

Система обробки та аналізу даних складається з центрального процесорного блоку, який збирає дані від усіх сенсорів, обробляє їх, фільтрує шуми, корелює інформацію та проводить первинну ідентифікацію об'єктів. Важливу роль відіграє програмне забезпечення з елементами штучного інтелекту (ШІ) та машинного навчання (МН). Воно здійснює розпізнавання образів, аналізуючи візуальні дані для класифікації БПЛА, аналізує радіочастотний спектр для виявлення характерних сигнатур управління та телеметрії, автоматично визначаючи частоти їхньої роботи та розпізнаючи відомі протоколи зв'язку. Також ПЗ прогнозує траєкторію руху об'єкта для оцінки потенційної загрози і, на основі отриманих даних та заданих алгоритмів, автоматично приймає рішення щодо необхідності активації засобів протидії. Система спирається на базу даних сигнатур БПЛА, що містить інформацію про радіочастотні характеристики, візуальні образи та акустичні сигнатури різних типів БПЛА, яка постійно оновлюється.

Система радіоелектронної боротьби (РЕБ) включає автоматичний пеленгатор частот, що швидко та точно визначає напрямок на джерело радіовипромінювання (БПЛА

та його оператора), та генератори електромагнітних перешкод (джамери). Джамери створюють потужні радіоелектронні перешкоди в діапазонах частот управління та навігації (GPS, ГЛОНАСС, Galileo, BeiDou), що призводить до втрати зв'язку між оператором та БПЛА, порушення його навігаційної системи і, як наслідок, до керованого приземлення, зависання або втрати орієнтації. Для мінімізації впливу на сторонні пристрої використовуються системи спрямованого випромінювання, що концентрують енергію перешкод у вузькому промені. Можуть також застосовуватися системи імітації сигналів - спуфінг, які генерують хибні сигнали GPS або управління, вводячи БПЛА в оману та змушуючи його відхилятися від курсу або сідати в заданій зоні. Опціонально можуть бути включені системи кібернетичного впливу, спрямовані на перехоплення управління БПЛА або впровадження шкідливого програмного забезпечення.

Система управління та оповіщення забезпечує операторський інтерфейс для візуалізації даних від усіх підсистем, відображення виявлених цілей, їхніх характеристик та статусу вжитих заходів. Автоматизовані протоколи реагування гарантують швидке та ефективне реагування на виявлені загрози відповідно до заданих алгоритмів. Система оповіщення інформує службу безпеки про виявлені загрози та вжиті заходи, що може включати звукові та світлові сигнали, повідомлення на пульти управління та мобільні пристрої.

Необхідна інфраструктура включає мережу сенсорів, розміщених по периметру та на території об'єкта для всебічного контролю повітряного простору, центральний пункт управління з обладнанням обробки даних, операторськими консолями та системами управління РЕБ, надійні канали зв'язку між усіма компонентами системи та гарантоване безперебійне електроживлення.

Перевагами такої автоматизованої системи захисту є висока швидкість реагування завдяки автоматичному режиму роботи без участі людини, можливість круглодобової роботи в будь-яких погодних умовах, висока ефективність завдяки комплексному використанню різних сенсорів та засобів РЕБ, що значно підвищує ймовірність успішної нейтралізації БПЛА. Також перевагами є мінімізація людського фактору, що знижує ризик помилок, адаптивність систем з ШІ/МН, які можуть навчатися та адаптуватися до нових типів БПЛА, та можливість легкої інтеграції з іншими системами безпеки, такими як відеоспостереження чи контроль доступу.

Однак існують певні складнощі та виклики при розробці та впровадженні таких систем. Необхідно розробити алгоритми та правила для розпізнавання "своїх" та "чужих" БПЛА та інтегрувати систему з обліком легальних польотів. Постійне вдосконалення технологій БПЛА вимагає регулярного оновлення програмного забезпечення та апаратних засобів системи захисту для протидії їхній еволюції. Важливо забезпечити стійкість системи виявлення та РЕБ до спроб створення навмисних радіоелектронних перешкод. Створення комплексної системи вимагає значних фінансових вкладень. Існують юридичні та етичні аспекти, пов'язані із застосуванням РЕБ у повітряному просторі та безпекою цивільних суден. Складність представляє інтеграція різнорідних сенсорів та систем в єдиний інформаційний простір, а також забезпечення кібербезпеки самої системи від атак та несанкціонованого доступу.

Перспективи розвитку включають подальше впровадження ШІ та МН для більш точної класифікації, ідентифікації БПЛА, прогнозування їхніх дій та автоматичного

вибору методів протидії. Можлива інтеграція з системами фізичного знищення (наприклад, сітками-пастками, лазерними установками), які активуються автоматично. Перспективним є створення мобільних комплексів РЕБ для оперативного розгортання, використання розподілених сенсорних мереж для раннього виявлення на великих відстанях, та розвиток пасивних методів виявлення БПЛА без активного випромінювання.

На завершення, автоматизована система захисту державних будівель від БПЛА різних типів за допомогою системи РЕБ з автоматичним виявленням частот управління та їх подавленням є перспективним та необхідним рішенням в умовах сучасних загроз. Її ефективність залежить від комплексності застосовуваних технологій, інтеграції різних сенсорів та систем, а також від постійного розвитку алгоритмів обробки даних та засобів протидії. Незважаючи на існуючі складнощі та виклики, подальший розвиток цієї галузі є критично важливим для забезпечення безпеки державних об'єктів та національної безпеки в цілому.

Толстоносов Юрій,
науковий співробітник НДЦ
службово-бойової діяльності НГУ,
Національна академія Національної гвардії України

Толстоносов Димитрій,
кандидат юридичних наук, доцент,
Київський інститут Національної гвардії України

АВТОНОМНІ СИСТЕМИ ОЗБРОЄННЯ: ПЕРЕВАГИ ЗАСТОСУВАННЯ В СУЧАСНИХ ВІЙНАХ ТА ВІЙСЬКОВИХ КОНФЛІКТАХ

Сучасне озброєння, яке поєднано із системами штучного інтелекту, серед військових фахівців має одну із назв – автономні системи озброєння (далі – АСО). На сьогоднішній день, якогось загальновизнаного формулювання чи визначення АСО поки що взагалі немає.

В той же час, у рамках міжнародної зустрічі експертів (13–16 травня 2014 року в Женеві), присвяченої бойовим автономним роботизованим системам (БАРС), учасники зустрічі визначили, що автономні системи озброєння (АСО) – це такі системи, які можуть самостійно, без контролю і втручання людини, виконувати наступні функції: пошук, виявлення, розпізнавання і ураження цілей.

Саме цим АСО і відрізняються від безпілотних літальних апаратів (БпЛА), яким обов'язково потрібна людина-оператор для вибору цілей, активації і наведення встановленої на них зброї, а також їх ураження (придушення). Але при цьому треба розуміти, що саме БпЛА є прототипами АСО – машин-роботів.

Повномасштабна війна, яка розпочалася в Україні 24 лютого 2022 р., значно прискорила процес вдосконалення АСО, що спроможні самостійно та ефективно виконувати службово-бойові (бойові) завдання за призначенням.

Використання АСО в сучасному світі стає важливим аспектом проведення військових операцій (бойових дій), оскільки вони поєднують в собі інформаційні дані, алгоритми дій, обчислювальну потужність та новітні зразки озброєння та техніки.

З початком російського вторгнення країни-партнери підтримали сили безпеки й оборони України та надали військову допомогу серед якої були деякі