DOI:**10.33099/2311-7249/2020-38-2-39-56**

УДК: 004.413.4

Сергій Григорович Вдовенко
Юрій Григорович Даник *(доктор технічних наук, професор)*
Олександр Юрійович Пермяков *(доктор технічних наук, професор)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

КІБЕРПРОТИДІЯ РОБОТОТЕХНІЧНИМ КОМПЛЕКСАМ

Стрімкий розвиток, масове виробництво, прийняття на озброєння та зростаюча кількість фактів бойового застосування у воєнних діях та конфліктах сучасності високотехнологічних систем озброєння та робототехнічних систем (комплексів) (РТС(К)) вимагають здійснення низки заходів щодо створення ефективної системи протидії РТК. Зокрема, розробки стратегій та концепцій, теорії та тактики протидії РТК, переосмислення канонів оперативного мистецтва та тактики застосування існуючих засобів ППО в контексті боротьби з РТС(К), вироблення вимог щодо модернізації та розвитку систем (комплексів) боротьби з РТС(К) (С(К)Б РТС(К)), проведення наукових досліджень, науково-дослідних та дослідно-конструкторських робіт щодо створення засобів та систем (комплексів) протидії РТС(К), організацію підготовки кваліфікованих спеціалістів з їх експлуатації та бойового застосування, науково-педагогічних кадрів, тощо. Враховуючи, що за своїми ознаками РТС(К) є кіберфізичними системами (КФС) спеціального призначення, а їх системи управління – класичними кібернетичними системами, пріоритетними є підходи щодо створення єдиних засад боротьби з РТС(К) (тих типів і класів, з якими неможливо або неефективно боротися існуючими засобами) та систем для їх реалізації, що складаються із органів управління та відповідно оснащених підрозділів, які мають на озброєнні системи (комплекси) ОВТ з специфічними програмно-апаратними засобами та комплекси для вирішення зазначених задач.

В статті представлені результати: аналіз ефективності застосування існуючих систем озброєння для боротьби з безпілотними літальним апаратам (БПЛА) поля бою безпілотних авіаційних комплексів (БАК); аналіз вразливості складових РТС(К); аналіз тенденцій розвитку систем (комплексів) боротьби з РТС(К) (БПЛА БАК) провідних країн світу в контексті можливості та доцільності впровадження їх досвіду в Україні; здійснення розробки основних теоретичних положень формування систем кіберпротидії РТС(К) як КФС.

Ключові слова: *безпілотні авіаційні комплекси (БАК); безпілотні літальні апарати (БПЛА); бойове застосування робототехнічних систем (комплексів); виявлення робототехнічних комплексів (засобів); кіберсистеми; кіберфізичні системи (КФС); робототехнічні системи (комплекси) РТС(К); системи (комплекси) боротьби з робототехнічними системами (комплексами) С(К)Б РТС(К)).*

Вступ

Постановка проблеми. В сучасних війнах та військових конфліктах значно зросли важливість та масштаби застосування високотехнологічних систем озброєння та робототехнічних комплексів (РТК), які вже стали обов'язковою складовою озброєння армій провідних країн світу Відбувається інформатизація та роботизація військових формувань. У збройних силах багатьох країн світу створюють роботизовані підрозділи які, відповідно до цього, вимагають розвитку форм, способів і засобів ведення боротьби з ними. У 2015 р. Російська Федерація у ході командно-штабного навчання "Центр-2015", а у 2016 р. Велика Британія в ході військових навчань НАТО Unmanned Warrior 2016 ("Безпілотний воїн"), що були складовою найбільших у Європі військових навчань Joint Warrior) провели тренування з комплексним використанням роботів (повітряного, наземного та морського базування) та інших інноваційних розробок із застосуванням високо інтегрованих систем управління [1-3].

РТС(К) є сукупністю: апаратних засобів робототехнічних засобів (РТЗ) (наземних, повітряних, надводних, підводних тощо);

програмно-алгоритмічних комплексів;

систем управління, що забезпечують комплексну (дистанційну, автономну або змішану) автоматизацію виконання задач.

Фактично, будь-яка робототехнічна платформа, яка є носієм цільових систем і засобів, являє собою механізм, що контролюється або відстежується комп'ютерними алгоритмами і (у разі, якщо він не є цілком автономним), пов'язаний з пунктом управління (ПУ) та його користувачами. При цьому бортовий апаратно-програмний комплекс, який забезпечує її застосування, здійснює процеси отримання даних, їх обробки, збереження та обміну ними, а також здійснює управлінські впливи на бортові виконавчі засоби та цільові системи, які взаємодіють на різних часових та просторових рівнях та можуть мати різні, відмінні одна від одної моделі поведінки та взаємодіяти

одна з одною різними шляхами, які можуть змінюватися в залежності від контексту. Це є прямими ознаками будь-яких кібернетичних систем та є характерним для систем кіберфізичних. Особливістю робототехнічних систем (комплексів) (РТС(К)) є поєднання усіх функціональних і структурних елементів у єдину складну кіберсистему, що має свою мету, функції, завдання, структуру, функціональні та зворотні взаємозв'язки і можливості до адаптації. З точки зору теорії систем вони є складними багаторівневими ієрархічними системами з їх функціями, елементами та взаємозв'язками.

Таким чином, за своїми ознаками РТС(К) є кіберфізичними системами (КФС) спеціального призначення [9-11], а їх системи управління – класичними кібернетичними системами [4-8].

Процеси функціонування таких систем відбуваються одночасно у природніх (сухопутному, морському, повітряному, космічному) просторах та у новому штучно утвореному віртуальному просторі – кіберпросторі, який доповнив існуючи та став сферою конфліктів і можливих бойових дій [12,13]. При цьому відбувається зміна традиційних форм і способів ведення протиборства.

Розглядаючи сферу оборони (військовий аспект), визначимо, що кіберпростір – це єдиний простір сформований з інформаційного, комунікаційного, віртуального комп'ютерно-мережного і соціотехнічного просторів та об'єднаний системою зв'язків, в якому відбувається створення, зберігання, модифікація та передача інформації, управління об'єктами (системами) та зброєю, вплив на об'єкти (системи) протидіючої сторони, захист власних об'єктів (систем) в існуючих фізичних полях та середовищах. З його утворенням в системному контексті значно зросли можливості та ефективність застосування РТС(К). Надзвичайно важливим чинником, який обумовлює значне зростання їх ролі під час виконання військами різноманітних завдань є те, що застосування РТС(К) в збройних конфліктах дозволяє мінімізувати втрати особового складу та зробити дії військ більш ефективними і раптовими [14].

В операції Об'єднаних сил на території Донецької та Луганської областей, активні дії противника супроводжуються застосуванням безпілотних авіаційних комплексів (БАК) - "Орлан-10", "Груша", "Застава" (Bird Eye 400), "Форпост" ("IAI Searcher"), "Елерон", "Птеро", "Гранат-1", "Гранат-2", "Гранат-4", квадрокоптер "Гранат-6", "Тахіон" та інших з метою ведення розвідки, дорозвідки, здійснення цілевказівок, постановки завад, або для доставки засобів ураження (табл.1). БПЛА БАК несуть серйозну загрозу і, зазвичай, застосовуються комплексно, по 2-3 у групі. Найбільш розпосюдженною моделлю застосування є така: один апарат провокує протиборчу сторону на активність, другий веде розвідку з висоти 1000—1500 м, третій, який перебуває на висоті 4,5–5 км та більше – ретранслятор, який забезпечує управління та отримання розвідувальної, телеметричної і службової інформації на пункті управління БАК он-лайн. Часто в групах два апарати – розвідник та ретранслятор. Іноді до груп включають БПЛА, які виконують завдання РЕП. Для створення активних шумових перешкод на БПЛА-розвіднику може встановлюватися додаткове обладнання. Поодинокі БПЛА застосовуються на тактичному рівні для дорозвідки цілей, нанесення ураження об'єктам та особовому складу з використанням вибухових засобів та речовин. Особливо небезпечними є розвідувально-ударні та ровзвідувально-вогневі комплекси, у складі яких на Донбасі застосовуються БПЛА: "Орлан-10", "Елерон", "Гранат-6". Вони здатні виявляти цілі та з високою точністю, у режимі реального часу, корегувати вогонь ствольної або реактивної артилерії та інших засобів кінетичного впливу, сприяти підвищенню ефективності застосування засобів некінетичного впливу. Наприклад, комплекс РЕБ РБ-341В "Леєр-3", до складу якого входять 3 БПЛА "Орлан-10" ("Орлан-30"), крім виконання основних функцій – виявлення, придушення та імітації роботи станцій діапазонів GSM 900, 1800, 2000, 2500, спроможний в режимі on-line передавати артилерійським підрозділам для нанесення вогневого удару інформацію щодо координат виявлених абонентських точок.

З початку збройного конфлікту на сході України, станом на липень 2020 р., підтверджено знищення понад 40 БПЛА РФ. В табл. 2 представлені зведені дані щодо деструктивного впливу на БАК РТС(К) ЗС РФ. Дані щодо впливу противника на українські БПЛА у відкритих джерелах відсутні. Разом з тим, за цей період з боку 1, 2 армійських корпусів РФ зафіксовано понад 10 випадків перешкоджання виконання завдання безпілотниками ОБСЄ, з яких не менш двох – з втратою БПЛА.

Аналіз інформації табл.1 свідчить що деструктивний вплив на БАК (РТС(К)) противника можливий шляхом застосування існуючих засобів, що перебувають на озброєнні ЗС України. Разом з тим, боротьба з БПЛА противника здійснюється наразі безсистемно і з різним ступенем ефективності.

При цьому, якщо боротьба з бойовими БПЛА стратегічного, оперативного і навіть деякими типами тактичного рівня є питанням в достатньому ступені відпрацьованим, то протидіяти невеликим БПЛА (класів мікро-, міні-, апаратів поля бою та їм подібних) (табл.2), як суто військового призначення, так і цивільним і кустарно виготовленим, сучасними засобами ППО складно, дорого і в багатьох випадках неефективно.

Слід відмітити, що до початку бойових дій не були належним чином оцінені загрози від РТК та вжиті відповідні управлінські рішення щодо розвитку засобів і створення систем протидії їм.

Проведений аналіз і дослідження показали, що підвищення ефективності протидії БПЛА можливе за рахунок не лише збільшення масової частки існуючих, в т.ч. сучасних зразків озброєння, але насамперед, створення та розвитку комплексної системи протидії БАК, як КФС, з використанням засобів кібервпливу [15,16] (на елементи та процеси управління з метою його порушення), фізичного (вогневого, енергетичного) впливу, а також утворення підсистеми виявлення – розпізнавання – супроводження – визначення найбільш раціонального виду впливу. Захист від мікро- та міні-БПЛА об'єктів протидії на власній території (органи військового управління, військові частини, арсенали, бази, склади) вимагає також утворення підсистеми оперативно-розшукового забезпечення із залученням структур сил безпеки держави.

Таблиця 1

РТК (БАК), БПЛА Російської Федерації, що застосовуються на Сході України

Назва, призначення,склад РТК (БАК)	Характеристики БПЛА		Оснащення, спроможності
Форпост (IAI Searcher) - розвідувальний оперативно-тактичний комплекс. БПЛА Форпост. Склад: станція управління, БПЛА - до 3.	Практична стеля, м	5800	Комплекс MOSP (Multimission Optronic Stabilised Payload) TV/FLIR з системою передачі для GCS в реальному часі або розвідувальним контейнером з радаром з синтезованою апертурою (SAR). Може комплектуватися кольоровою CCD відеокамерою.
	Максимальна швидкість, км/год	150	
	Практична дальність, км	250	
	Тривалість польоту, год	17	
Форпост (Searcher II) - розвідувальний оперативно-тактичний комплекс. БПЛА Форпост-Р. Склад: станція управління, БПЛА - до 3.	Практична стеля, м	7010	
	Максимальна швидкість, км/год	200	
	Практична дальність, км	250	
	Тривалість польоту, год	15-18	
Леер-3 - комплекс РЕБ РБ-341В. Склад: базова станція (робочі місця операторів, радіообладнання управління і передачі даних), обладнання для технічного обслуговування і забезпечення старту БПЛА, бензоагрегат, БПЛА Орлан-10 (30) – до 3.	Практична стеля, м	5000	Корисне навантаження: Орлан-10 – 12 камер., Орлан-30: фотокамери (роздільна здатністю10-15 Мрх, кратність х 4 – 8) – 7; відеокамери – 10: курсові – 3, планові -3, поворотні -2, гіростабілізоівні – 2; тепловізори (чуйність 0,005С° , дальність розпізнавання людини – 450 та 1150м. Можливості: одночасне управління з ПУ – до 4 БПЛА, будь-якій БПЛА – ретранслятор; організація локальної мережи до 30 операторів для управління корисним навантаженням одночасно запущених БПЛА.; створення карти місцевості в 3D і управління ходом бою.
	Максимальна швидкість, км/год	150	
	Практична дальність, керування дистанційне (автономне), км	120 (600)	
	Тривалість польоту, год	16	
Орлан-30 - Розвідувально-тактичний БПЛА	Практична стеля, м	5000	
	Максимальна швидкість, км/год	150	
	Практична дальність, км	500	
	Тривалість польоту, год	8-12	
Груша - малогабаритний розвідувальний комплекс. Склад: станція управління, 3 БПЛА, катапульта, комплект корисного навантаження (фото, відіео).	Практична стеля, м	3000	Корисне навантаження: радіообладнання, фотоапарат (роздільна здатність10Мрх, кратність – 4, відеокамери (здатність 720х576 рх) – 2. Здатний з висоти 300-500 м виявляти замасковані об'єкти на відстані до 15 км, корегувати вогонь РСЗВ, фіксувати результативність вогню.
	Максимальна швидкість, км/год	120	
	Практична дальність, км	5-10	
	Тривалість польоту, год	1,25	
Застава - тактичний безпілотний авіаційний комплекс, БПЛА - Застава (Bird-Eye 400). Склад: переносний пункт управління, комплекс зв'язку, цільова оптико-електронна апаратура, БПЛА - 3.	Практична стеля, м	2200	Корисне навантаження: або TV, або ІЧ-камера на гіростабілізованій платформі, що обертається. Здатний вести розвідку та корегувати вогонь артилерії на відстані прямого бачення.
	Максимальна швидкість, км/год	120	
	Практична дальність, км	10	
	Тривалість польоту, год	1	
Гранат-4 Комплекс дистанційного спостереження і ретрансляції. БПЛА Рубеж-20. Склад: кБомплеекс наземних засобів управління, транспортно-пусковий комплекс, БПЛА. – 2	Практична стеля, м	4000	Корисне навантаження: або TV, або ІЧ-камера, або фотокамера, або блок РЕБ. Здатний вести спостереження та передавати інформацію на відстані до 100 км .
	Максимальна швидкість, км/год	140	
	Практична дальність, км	100	
	Тривалість польоту, год	6	
Гранат-1. Переносний комплекс дистанційного спостереження і ретрансляції. БПЛА - Гранат-1. Склад: Станція управління, комплект змінних модулів корисного навантаження, БПЛА - 2.	Практична стеля, м	3500	Корисне навантаження: або TV, або ІЧ-камера, або фотокамера. Здатний з висоти 1500 м виявляти цілі на відстанідальности до 15 км та надавати цілевказання до розвідувально-вогневих комплексів.
	Максимальна швидкість, км/год	75	
	Практична дальність, км	15	
	Тривалість польоту, год	1,4	

Таблиця 2

Класифікація БПЛА

За масштабом завдань, що вирішуються		Приклад	радіус дії (км)		Маса (кг)		тривалість польоту (год)		практична стеля (км)	
тактичні (Tactical Unmanned Aerial Vehicles)										
Тактичні	Нано-БПЛА	Perdix	Поля бою	до 1	Нано- (Nano, η)	до 0,025	Малої тривалості (short duration)	до 1	Маловисотні (low altitude)	до 1
	Мікро-БПЛА (Micro Air Vehicle)	Т-4 Елерон		до 10	Мікро- (Micro, μ)	до 5		1-1,5		1 -2
	міні-БПЛА (Mini Air Vehicle).	Груша Застава Bird-Eye 400		5-15	Міні- (Mini)	до 15		до 2		1 - 4
	ближньої дії (close range)	Тахіон Птеро	Ближнього радіусу	30-70	Мало-розмірні	25–150		2-4		4 - 6
	малої дальності (short range).	RQ-7 Shadow	Малого радіусу	до 100	Середньо-розмірні	до 250		4 - 8		
з великою тривалістю польоту EUAV (Endurance Unmanned Aerial Vehicles)										
Оперативно-тактичні	середньої дії (medium range)	Ту-141 (Стриж) Форпост IAI Searcher Bayraktar Anka Орлан-10	Середнього радіусу (Medium Endurance)	до 200	Велико-розмірні	до 500	Середньої тривалості (medium duration)	6 - 12	Середньо-висотні (medium altitude).	4 - 8
Оперативні	великої дальності (long range)	MQ-1 Predator Ту-243(Рейс) Орлан-30		до 700		500 – 1500	Великої тривалості (long duration)	понад 12		6 - 12
Оперативно-стратегічні (MALE - Medium Altitude, Long Endurance)		Оріон Bayraktar TB2	Дальнього радіусу (Long Endurance)	понад 800	Важкі	1000 - 1500		понад 20.	Висотні (high altitude)	4 - 12
Стратегічні (HALE - High Altitude, Long Endurance)		RQ-4 Global Hawk MQ-9 Reaper		понад 2000		2500 - 5000		понад 30	Стратосферні (stratospheric)	понад 12

В основу класифікації, прийнятій в НАТО, покладено поділ БПЛА за висотою і тривалістю польоту. Крім того класифікувати військові БПЛА доцільно за:
функціональним призначенням (характером завдань) - розвідувальні, ударні, радіоелектронної боротьби, ретранслятори зв'язку;зв'язку, управління, комбіновані;
за технічними ознаками: принципом керування – дистанційно пілотовані, автономно (за програмою), комбіновано пілотовані,. дистанційно керовані авіаційною системою short range Air Vehicle

Таблиця 3

Дані щодо ураження БПЛА РФ на Сході України

кіль к	тип	од	виявлено	вплив
2014				
7	IAI Searcher	2	В	АЗ
	Орлан-10	5		
2015				
8	IAI Searcher	1	В	АЗ
	Орлан-10	3	В - 2	АЗ
			НВ - 1	РЕП
	Форпост	2	В	АЗ
	Застава	2	В-1	АЗ
			КПЗТР-1	ЗУ
2016				
2	Орлан-10	2	В - 1	АЗ
			КПЗТР-1	ЗУ
2017				
4	Орлан-10	3	В - 2	АЗ
			КПЗТР-1	ЗУ
	Гранат-1	1	В	АЗ
2018				
9	Орлан-10	9	РЛС - 8	ППО-7
				Мі-24-1
			КПЗТР-1	ЗУ
2019				
11	Гранат-2	1	КПЗТР	ЗУ
	Елерон	2	В	АЗ
	Фантом-4	1	В	АЗ
	Орлан-10	2	В	АЗ
	Гранат -6	4	КПЗТР	ЗУ
	саморобний	1	КПЗТР	ЗУ
2020 (перше півріччя)				
2	Орлан-10	1	В	АЗ
	Застава	1	КПЗТР	ЗУ

(В – візуально, НВ - не виявлено, КПЗТР – комплекс перешкоджання повітряним та наземним засобам технічної розвідки "Нота", РЛС – радіолокаційні засоби, АЗ – автоматична зброя, РЕП – радіо-електронне подавлення, ЗУ – захоплення управління, Мі-24 – гелікоптер, ППО - засоби ППО, цифрами вказана кількість БПЛА).

Проблема боротьби з РТС(К) противника є надзвичайно актуальною і вимагає якомога швидшого вирішення, для чого необхідне комплексне залучення наявного наукового та технічного потенціалу держави.

Зважаючи на це, крім розвитку форм і способів застосування власних РТК (БАК тощо) постає питання ефективної протидії аналогічним системам (засобам) противника. Тому в провідних країнах світу проводяться інтенсивні дослідження в цій сфері. Розроблені інноваційні та існуючі організаційні заходи, системи (комплекси) дозволяють в певному сенсі вирішувати зазначені питання, але необхідний рівень ефективності, як в організаційному, так і технічному плані, і досі не забезпечений. В Україні також проводяться заходи щодо дослідження і розробки засад та комплексів (засобів) боротьби із РТС(К) та РТЗ РТС(К) [14,18,19].

Аналіз останніх досліджень і публікацій. У теоретичному і практичному плані питання кібервпливів на кіберсистеми РТЗ розглянуті у відомих роботах Алмазова В.Д, Вакіна С.А., Максимова М.В., Палія А.І., Цурского Д.А. Значна кількість вітчизняних та зарубіжних фахівців пропонує здійснювати боротьбу з РТК шляхом виявлення та фізичного знищення цілі, або шляхом постановки широкосмугових завад [20-22].

Фахівці Військової академії військової ППО ЗС РФ імені А. М. Василевського та Харківського Національного університету Повітряних Сил ім. Івана Кожедуба, до складових частин системи протидії міні- та мікро-БПЛА відносять "активну" (вогневе ураження БПЛА в повітрі й на землі) та "пассивну" (невогневу). Для створення останньої вважається за необхідне, між іншим, вжиття комплексу заходів з протидії системам розвідки, управління та бойового застосування БПЛА, а також розробка спеціалізованих, заснованих на нетрадиційних способах ураження, засобів й комплексів протидії малорозмірним цілям. До останніх відносять засоби кінетичного ураження: лазерні та мікрохвильові (НВЧ)-гармати, дрони-"камікадзе", а також ручні засоби нейтралізації безпілотних літальних апаратів, виготовлені у вигляді гвинтівок [23,24].

Стратегія протидії БПЛА МО США ("The DOD's counter-unmanned aircraft system (C-UAS) Strategy") визначає комплекс організаційно-правових, режимно-обмежувальних, науково-технічних та безпосередньо воєнних заходів. Зазначається необхідність організації взаємодії з іншими федеральними інституціями, а також збройними силами країн-партнерів, в т.ч. у випадку ведення коаліційних воєнних дій. Звертається увага на забезпечення США та союзниками збереження в таємниці інформації щодо сучасних технологій, яка може надати імовірному противнику змогу у створенні перспективних БПЛА. Вказується на необхідність об'єднання усіх видів озброєння різних родів військ та скоординованого використання в операціях їх інформаційних та вогневих спроможностей, у поєднанні з обов'язковим виконанням заходів маскування від БПЛА-розвідників. Значна роль у протидії БПЛА визначається Кіберкомандуванню США та підрозділам радіоелектронної протидії. В короткостроковій (2020) перспективі Стратегія передбачає використання армійських та об'єднаних мереж обміну необхідною інформацією з підрозділами рівня взвод-рота. В довгостроковій (2025) – створення автоматизованої системи розподілу такої інформації до окремих військовослужбовців. Метою заходів визначена швидка й, так звана, безшовна інтеграція (розробка алгоритму обміну необхідними даними у зручних для споживання формі та форматі) усіх спроможностей та об'єднання зусиль щодо розробки й розгортання систем протидії БПЛА. Основні зусилля утворення таких систем направлені на модернізацію існуючих систем: управління (командних пунктів); виявлення; ідентифікації, в т.ч. державного впізнавання; протидії. Алгоритми протидії,

включно фізичне ураження, мають забезпечити швидке та гарантоване ураження БПЛА противника та уникнення ураження власних дронів. При цьому, в Стратегії згадується про те, що підрозділи Армії США досі використовують візуальне та/або акустичне виявлення БПЛА. Тому, Стратегією сформульоване завдання щодо об'єднання радіоелектронних, оптоелектронних, інфрачервоних та акустичних сенсорів в єдину систему, що має бути інтегрована до єдиної системи $C^{X}ISR$ мережецетрічної платформи управління воєнними діями NCW (Network-centric Warfare), наприклад у варіантах: C6ISR (Command, Control, Communication, Computers, Combat System, Cyber, Intelligence, Surveillance, Reconnaissance), або C5IEWS&IM (Command, Control, Communications, Computers, Cyber, Intelligence, Electronic Warfare, Sensors and Information Management). Що дозволятиме автоматизованій системі та/або людині визначати тип БПЛА й задіяти/запропонувати варіанти застосування засобів впливу або ураження. На виконання Стратегії Пентагон визначив завдання створення 2-5 систем, які найбільш будуть придатні для протидії БПЛА та можуть бути застосовані за призначенням в усіх видах Збройних Сил. Визначено спектр технологій протидії БПЛА. Враховуючи розвиненість систем ППО, здатних протидіяти важким БПЛА, пріоритетними у розвитку систем протидії малим БПЛА, визнані технології: придушення систем БПЛА (EnforceAir C-UAS (counter-unmanned aircraft system)), та вдосконалена протидія малим БПЛА (D-Fend EnforceAir advanced C-sUAS (counter small unmanned aerial systems)). Система C-UAS – це вдосконалена автономна система, призначена для автоматичного виявлення, ідентифікації, визначення просторових параметрів БПЛА з наступним перехопленням управління ними та примусу до приземлення у безпечній зоні, або до відмови від виконання ними польотного завдання. Виявлення цілі передбачається здійснювати з використанням: 1) оптоелектронних, інфрачервоних та акустичних засобів; 2) радіолокаційних систем; та, з урахуванням проблем виявлення першими двома способами нано-, мікро- та міні-БПЛА, 3) радіочастотних датчиків бездротових сигналів, що використовуються для управління останніми. Ці методи мають поєднуватися, щоб забезпечити більш ефективне виявлення. Дана технологія не передбачає встановлення широкосмугових завад або кінетичного ураження на відстані прямого бачення, натомість передбачає перешкоджання роботі електронних, електронно-механічних та кіберсистем БАК. Перспективними вважаються: НВЧ- та акустичні (на резонансних частотах гіроскопів) удари, а також спуфінг-атаки - нав'язування БПЛА хибної командної та геонавігаційної інформації (GPS-спуфінг).

Технологія C-UAS не виключає також нейтралізацію БПЛА за допомогою традиційних систем ППО, спрямованої енергії, механічних перешкод (сіток), дронів-камікадзе, або навіть таких екзотичних, як навчені птахи (орли).

На виконання завдань Стратегії:

визначені спонсори (замовники) для протидронних систем: стаціонарних та портативних – види ЗС (US Army, US NAVY, US Air Force), для мобільного – корпус морської піхоти (US Marine Corps);

у 2019 р. на програму C-sUAS витрачено близько $900 млн., у 2020 р. на фінансування програми C-sUAS лише для Міністерства внутрішніх справ США передбачено $500 млн.;

у 2020 р. в інтересах МО США передбачено придбання та утримання однієї стандартизованої системи управління протидії БПЛА, 7 оборонних систем C-sUAS, понад 40 польових систем C-sUAS;

у 2021 р. МО (DOD) планує витратити щонайменше $ 404 млн на C-UAS дослідження та розробки та в щонайменше $ 83 млн на закупівлі C-UAS;

US NAVY спільно з командою DDS (Defense Digital Service), заснованою в Пентагоні у 2015 р. з метою впровадження сучасних науково-технічних рішень для посилення національної оборони, розпочав роботу з розробки програмного забезпечення з підтримкою кіберпрофілю систем C-UAS призначених для впливу на перспективні БПЛА;

у Крістал-Сіті штат Вірджинія поблизу Пентагону створено підрозділ чисельністю 60 оісб під керівництвом двозіркового генерала, відомий як Спільний офіс C-sUAS (JCO).

Армія США опублікувала власну Стратегію боротьби з БПЛА (US Army Counter-Unmanned Aerial Systems), яка основну роль в боротьбі з БПЛА визначає засобам ППО, але наголошує, що й інші підрозділи повинні бути здатними до їх виявлення та ураження. Підрозділи на полі бою мають бути здатні застосовувати власні засоби розвідки і впізнавання та обмінюватися з пунктами управління інформацією щодо будь-яких загроз від БПЛА. Зазначається, що загроз від БПЛА противника найкраще уникати шляхом превентивного знищення наземних станцій управління та операторів.

Для боротьби з БПЛА США розміщують на закордонних базах лазерні системи HELWS (High-Energy Laser Weapon System) з багато спектральними системами наведення HELWS (High-Energy Laser Weapon System), електромагнітні системи THOR та імпульсні системи PHASER. HELWS може робити кілька десятків пострілів на одному заряді та відрізняється підвищеною точністю. PHASER здатна виводити з ладу дрони за одну мікросекунду та дозволяє атакувати кілька цілей одночасно. Завдання електромагнітної системи THOR — знищення груп безпілотників. Системи випробовуються в бойових умовах на базах в Іраку

і Сирії, після чого будуть розміщені на базах у США.

По програмі D-Fend EnforceAir advanced C-sUAS США здійснює військово-технічне співробітництво з іншими країнами, зокрема – Ізраїлем. Дослідження та розробки з цього напряму здійснюються також у Великій Британії, Німеччині, Австралії, Канаді.

В провідних країнах світу здійснюється цілеспрямована робота щодо теоретичного обґрунтування, прийняття стратегій, концепцій, створення засобів цільового призначення протидії КФС. З метою підвищення рівня захищеності своїх КФС, а також збільшення рівня ефективності впливу на КФС противника, створюються науково-дослідні установи, як то Лабораторія кіберфізичних систем Академії ВМС США. Під патронатом та за фінансування Агентства передових оборонних дослідницьких проектів DARPA (Defense Advanced Research Projects Agency) МО США з 2012 р. здійснюється розробка стійких до кібервпливу БАК. В рамках програми HACMS (High-Assurance Cyber Military Systems), що буквально перекладається як високонадійні кіберсистеми військового призначення, розроблена операційна система seL4 з імітостійким ядром. Наприкінці 2019 р. компанії Rockwell Collins, Boeing и 3D-Robotics провели випробування квадрокоптера Iris и безпілотного гелікоптера Little Bird з таким програмним забезпеченням[25].

В РФ не розглядається питання щодо утворення окремої системи для боротьби з БПЛА БАК, які традиційно вважаються засобами повітряного нападу. Разом з тим, з 2016 р. малорозмірні БПЛА визнаються основними об'єктами ураження для підрозділів взвод-рота. Задачі з виявлення БПЛА в ЗС РФ виконують радіолокаційні та оптичні системи виявлення зенітно-ракетних комплексів, засоби РЕР тощо. Концепція боротьби з БПЛА визначає завдання щодо вдосконалення систем ППО та РЕБ. В т.ч. щодо створення гібридних комплексів ППО, призначених для протидії БПЛА. Вважається, що у перспективних комплексах, розміщених на одній платформі, будуть інтегровані: засоби радіоелектронних та оптоелектронних систем виявлення, різні типи озброєння, від засобів РЕБ та НВЧ-впливу до вогнепальної зброї. Створення лазерних систем боротьби з РТК в близької перспективі в РФ не розглядається з причин залежності від кліматичних умов, аерозольно-маскувальних спроможностей, та головним чином – потреби у великій енергетичної потужності, що наразі для РФ є невирішеним. Перспективні зразки мають ознаки кіберсистем.

На озброєнні російської армії перебуває декілька сучасних систем РЕБ, спеціально розроблених, або функціонально спроможних протидіяти БПЛА різних типів. Окремі з них (РБ-341В "Леєр-3", Р-330Ж "Житель",1Л269 "Красуха-2", "Репеллент-1", "Шиповник-АЭРО") пройшли бойові випробування в Сирії та Україні.

Р-330Ж "Житель" (на базі КамАЗ) – комплекс РЕБ, призначений для виявлення, пеленгування та радіоподавлення: базових станцій стандарту GSM 900/1800/1900; мобільних станцій супутникового зв'язку Inmarsat та Iridium; навігаційної апаратури користувачів систем супутникового зв'язку NAVSTAR (GPS). Ефективна дальність придушення – в радіусі 20-30 км. В ході випробувань та навчань "Щит Союзу-2015" застосовувався для протидії БПЛА.

1Л269 "Красуха-2" (3 автомобіля КамАЗ) – уніфікований наземний комплекс перешкоджання авіаційним РЛС (аналоговий) призначений для постановки активних перешкод і протидії бортовим радарам ударної, розвідувальної авіації та БПЛА в КХ та УКХ діапазонах, а також перешкоджання роботі транкінгового зв'язку. Радіус просторової дії 360°*180° не менш ніж 300 км. Комплекс здатний об'єднувати інші комплекси РЕБ та РЕР в єдину мережу, що значно підвищує ефективність застосування засобів.

1РЛ257 "Красуха-4" (2 автомобіля КамАЗ) – багатофункціональний мобільний комплекс радіоелектронного придушення (цифровий) з характеристиками аналогічними 1Л269.

"Репеллент-1" (на базі КамАЗ) – комплекс РЕБ з малорозмірними БПЛА оснащено потужною оптоелектронною системою кругового огляду з ІЧ-модулем, здатним виявляти цілі в будь-яких погодних умовах вдень і вночі, засобами РТР та РЕБ, з дальністю виявлення та впливу – до 30 км, та імітатором сигналів команд управління БПЛА.

"Шиповник-АЭРО" (на базі КамАЗ) – багатоцільовий комплекс РЕБ призначений для перехоплення управління БПЛА. Може бути застосований для придушення станцій телевізійних та радіомовлення, каналів зв'язку командних пунктів, мобільного зв'язку, Wi-Fi, WiMAX, DECT. Функції комплексу: автоматизований пошук цілей; виявлення; пеленгування; ідентифікація та визначення типів сигналів ліній управління БПЛА з дистанційним керуванням; формування каталогу частот; класифікація БПЛА; його захоплення та супроводження; аналіз та визначення характеристик каналів управління БПЛА; придушення каналів управління. Придушення здійснюється шляхом комплексного застосування трьох методів: 1) блокування перешкодами каналу GPS-навігації; 2)безпосереднє придушення каналу управління БПЛА; 3) перехоплення управління БПЛА за рахунок імітації хибних сигналів в каналі управління.

Комплекс забезпечує широкосмугове та вузько направлене придушення сигналів та частот, викривлення інформації первинного джерела в тракті приймача. Здатний виявляти та ідентифікувати сигнали управління БПЛА в радіусі до 10 км. На підставі аналізу параметрів цілі обирається найбільш ефективний тип

перешкоди. Спроможний зламати коди управління бортових систем БРЛА та взяти під контроль управління ним.

“Луч-ПРО” – стаціонарний комплекс протидії БПЛА направленої дії призначений для цілеспрямованого впливу на канали управління, навігації та передачі інформації БПЛА, приведення їх у неробочий стан з метою перешкоджання функціонування БПЛА в повітряному просторі об’єкту, що захищається. Радіус дії - до 6 км.

“Купол-ПРО” – переносний комплекс протидії БПЛА призначений для захисту важливих об’єктів шляхом загороджувального електромагнітного впливу на бортові радіоелектронні системи БПЛА та приведення їх у неробочий стан. Радіус просторової дії 360°*180° не менш ніж 2,5 км.

“Пищаль-ПРО” – портативна система протидії, призначена для цілеспрямованого впливу на канали управління, навігації та передачі інформації БПЛА з метою зриву його польотного завдання. Маса – 3 кг. Дальність ефективної протидії – 2,5 км.

“Таран-ПРО” – переносний комплекс протидії БПЛА для впливу на канали управління, навігації декільком БПЛА. Дальність придушення каналів управління та навігації – 2,7 км. Є ефективним у разі масованого нападу БПЛА з кількох напрямів. При їх виявленні комплекс створює над об’єктом, що захищається захисний “купол” радіусом не менш ніж 900 м.

“Рубеж-Автоматика” - перспективний переносний комплекс протидії БПЛА з елементами штучного інтелекту, здатний виявляти та нейтралізувати БПЛА без участі людини. До складу комплексу входять засоби радіолокаційного та оптоелектронного виявлення, радіотехнічної розвідки та адаптивні засоби радіоелектронного придушення.

“Палантин-К” – перспективний оперативно-тактичний мобільний комплекс РЕБ нового покоління призначений для ведення радіоелектронної розвідки та придушення в КХ- та УКХ-діапазонах існуючих та перспективних систем зв’язку, які побудовані на платформі SDR (Software-defined radio – програмно визначаємо радіосистема), а також утворення перешкод мобільному та транкінговому зв’язку.

Комплекс здатний об’єднувати різні комплекси РЕБ та РЕР в єдину бойову мережу, що значно підвищує ефективність їх застосування. В ньому реалізована сучасна система підтримки прийняття рішення, що дозволяє без участі оператора обирати оптимальний алгоритм виконання задачі, оптимально розподіляти ресурси та функціональне навантаження кожної з машин. Після успішного завершення військових випробувань “Палантин-К” поступив на озброєння Західного ВО ЗС РФ.

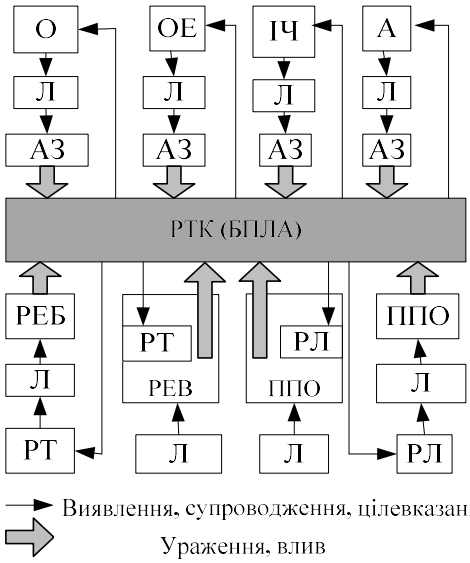
“Егида” – перспективний комплекс боротьби з БПЛА, що створюється на базі розроблених та випробуваних зразків озброєння, таких як:

пасивний когерентний локатор (ПКЛ) призначений для виявлення рухомих об’єктів, в т.ч. таких, що не використовують GPS, за сигналами, які відбиваються,. Не має демаскуючого випромінювання та є ефективним навіть в умовах міста;

модуль радіомоніторингу “Черемуха” призначений для встановлення факту обміну інформацією між виявленим та іншим об’єктом, ідентифікації об’єкт як БПЛА, прогностичного визначення місця знаходження пункту керування з похибкою 2 град.;

модуль радіоелектронного придушення “ Серп” призначений для автоматичного супроводження БПЛА та перешкоджання роботі його системам управління та зв’язку шляхом придушення сигналів GPS и ГЛОНАСС (L1, L2, L5), GSM900, Wi-Fi. Дальність ефективної протидії – 20 км.

Тактико-технічне завдання на комплекс “Егида” передбачає його спроможність виявляти та перешкоджати роботі БПЛА що використовують криптографічно захищені канали обміну інформації. Спеціальне програмне забезпечення комплексу дозволяє визначити тип БПЛА (літаковий, гелікоптер ний, аеростатичний) та спрогнозувати траєкторію його приземлення після придушення сигналів управління [26].



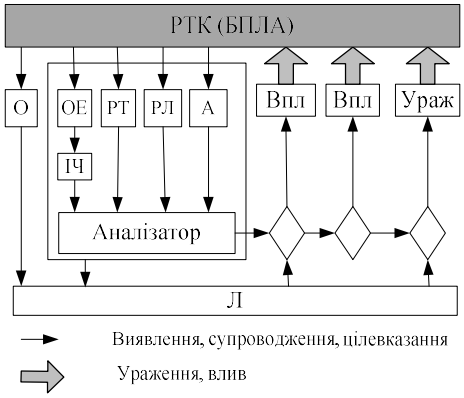
(Л – людина; засоби виявлення: О – оптичні ОЕ – оптоелектронні, ІЧ – інфрачервоні, А – акустичні, РТ – радіотехнічні, РЛ – радіолокаційні; засоби впливу: РЕВ – радіоелектронного ППО – засоби ППО, АЗ – автоматична зброя,)

Рис. 1.Схема застосування наявних засобів виявлення та протидії (ураження) БПЛА

В Україні для протидії БПЛА використовуються окремі можливості існуючих в т.ч. деяких новітніх зразків озброєння (рис.1). При цьому, розробляються і впроваджуються не стратегії та концепції, а лише окремі елементи засад, форм, способів, методів, тактики бойового застосування окремих існуючих, не зведених у бойову систему, засобів протидії. Однак, з урахуванням недостатньої кількості діючих

засобів протидії РТС(К) противника з одного боку та їх недостатньою ефективністю і малими ресурсними можливостями з іншого, проблема утворення та бойового застосування систем комплексної кіберпротидії РТС(К) противника досі залишається невирішеною.

До теперішнього часу протидія БПЛА розглядалася як боротьба із засобами повітряного нападу. Дослідження останнього часу свідчать про доцільність та необхідність вирішення проблеми шляхом створення спеціалізованих систем боротьби з РТС(К) та РТЗ РТС(К) противника для забезпечення їх своєчасного виявлення, ідентифікації та протидії їм як КФС. Тому, пріоритетними є підходи щодо створення єдиних засад боротьби з РТС(К) (тих типів і класів, з якими неможливо або неефективно боротися існуючими засобами) та систем для їх реалізації, з органами управління та відповідно оснащеними підрозділами, які мають у своєму складі специфічні технічні засоби для вирішення зазначених задач.



(Впл – засоби впливу, Ураж – засоби ураження)

Рис. 2. Перспективна схема побудови системи комплексної протидії РТС(К) (БПЛА)

Характерною рисою підходів, які розглядаються, є комплексність використання засобів виявлення, видачі цілевказівок, наведення та ураження, кібервпливу на функціональні системи РТС(К), які функціонують на різних фізичних принципах. Комплексність та системність при цьому забезпечується шляхом об'єднання інформаційних потоків, сумісної обробки отриманих даних про типи об'єктів, їх окремі характеристики, стан функціонування РТС(К) противника, виявлення в РТК вразливих елементів та зв'язків між ними, здійснення розподілено-зосередженого кібервпливу з метою зміни параметрів функціонування РТС(К), перехоплення управління ним, досягнення запуску деструктивних ланцюгових ефектів в процесі комплексного впливу [16] (рис.2).

Враховуючи це, **метою статті** є розробка обґрунтованих підходів та формування засад раціонального бойового застосування засобів комплексної кіберпротидії кіберсистемам РТС(К) противника.

Виклад основного матеріалу дослідження.

В статті модель РТС(К) противника буде розглядатися на прикладі безпілотних авіаційних комплексів (БАК), як таких, що знайшли широке застосування в бойових (воєнних) діях сучасності.

Безпілотний РТС(К) (рис.3) у мінімальній конфігурації включає до свого складу:

платформу-носій (наземну, повітряну, морську) з цільовою апаратурою, бортовими системами прийому/передачі даних, системою керування та іншими апаратними засобами:

наземний, бортовий: корабельний або повітряний віддалений комплекс управління (ВКУ), з комплектом апаратури, який складається з антенної системи (систем), програмно-апаратних комплексів для виконання завдань: управління безпілотним апаратом, корисним навантаженням та обробки інформації;

зовнішні системи інформаційного забезпечення РТК;

зовнішні системи його обслуговування та забезпечення бойового застосування.

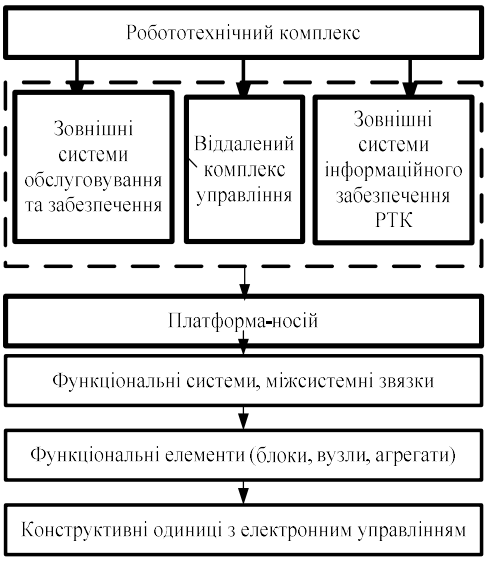


Рис 3. – Структура безпілотного РТС(К).

Бортова складова підсистеми управління представляє собою сукупність функціональних вузлів (окремих систем) і містить інерціальні навігаційні засоби; засоби автономного керування (за програмою); засоби дистанційною (ручного) керування. До складу обов'язкового бортового обладнання БПЛА входять бортова електронно-обчислювальна машина або спеціальні обчислювачі чи спеціальні процесори, приймач сигналів радіонавігаційної системи, висотомір, гіровертикаль, сервомеханізми, бортові сенсори для забезпечення польоту, енерго-силове обладнання, приймально-передавальну апаратуру, засоби безпечного запуску та посадки, рульові машинки.

Функціональна схема бортового обладнання безпілотного апарату, наземної (бортової) системи управління та обробки сигналів, наведена на рис. 4.

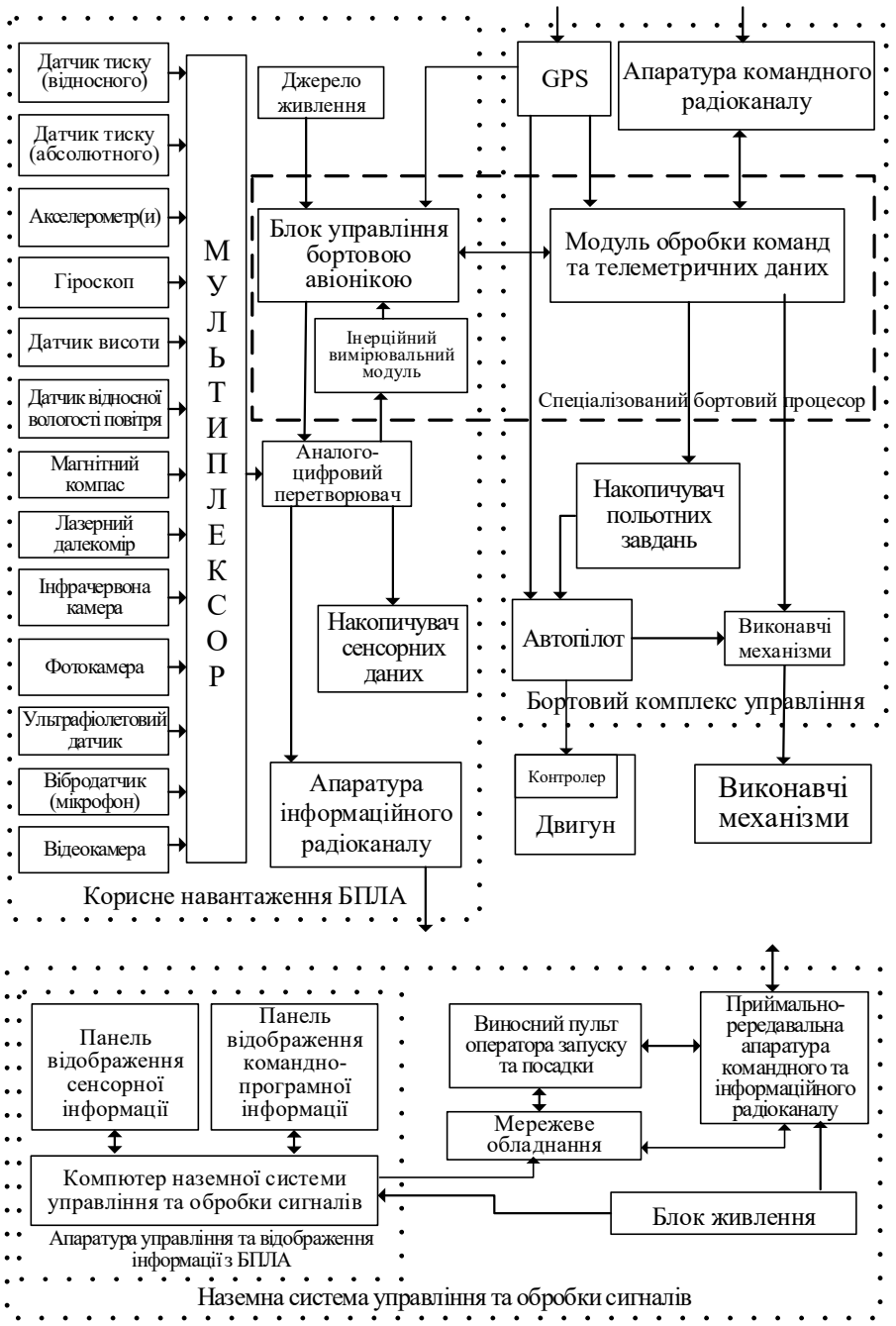


Рис 4 - Функціональна схема бортового обладнання БПЛА, наземної системи управління та обробки сигналів

Віддалений відео термінал (ВВТ; від англ. RVT – Remote Video Terminal) – портативна система, призначена для прийому і відображення розвідувальної інформації та телеметрії з борту БПЛА. ВВТ може приймати радіосигнал власною антеною або через апаратні засоби ВКУ.

Підсистема зв'язку (прийому та передачі даних) з БПЛА, як правило, складається з двох радіоканалів: командного та інформаційного, утворених відповідними радіолініями і апаратурою прийому, обробки і передачі даних.

Командний радіоканал призначений для передачі сигналів керування з ВКУ на бортову апаратуру БПЛА з метою його маневрування, зміни висоти, курсу, швидкості польоту, режимів роботи розвідувальної та іншої апаратури. Дальність прийому УКХ сигналів на частотах 910–920 МГц становить біля 10–15 км

Телеметричний канал призначений для обміну інформацією щодо просторового положення, стану систем та керованості об'єкту (БПЛА).

Інформаційний канал використовується для передачі в КХ та УКХ діапазонах, з використанням супутникового зв'язку тощо, інформації від бортових систем корисного навантаження БПЛА на ПУ. Як правило,

інформаційний і телеметричний канали об'єднані в один зворотний радіоканал.

Для обміну інформацією між декількома БПЛА застосовуються радіомодеми, які відрізняються між собою вихідною потужністю (для передатчиків), чутливістю (для приймачів), робочим діапазоном частот, споживаною потужністю та швидкістю передачі даних.

Вирішуючи завдання забезпечення функціональної стійкості та функціональної спроможності РТС(К), що виконує завдання в умовах апріорної невизначеності, розробник (противник) буде намагатися побудувати систему комплексного захисту РТС(К), на принципах доцільності, раціональності та розумної достатності. Такі системи створюються з урахуванням наступних основних вимог:

безперервність функціонування;

комплексність (реалізація організаційних, організаційно-технічних й інженерно-технічних засобів та заходів);

уніфікація програмно-апаратних та алгоритмічних рішень систем захисту;

автономність функціонування технічної компоненти системи захисту;

реалізація багаторівневої системи контролю безпеки та захисту від помилок персоналу;

забезпечення обмеження кола осіб щодо виконання ними повноважних функцій;

дотримання розумного балансу між завданням швидкої обробки великих обсягів інформації в системі за мінімальний наявний проміжок часу та необхідністю витрачання значного ресурсу на досягнення мети функціонування систем захисту;

забезпечення багаторівневого захисту відповідно до загроз [27-30].

Спрощено модель загроз РТС(К) КФС може бути представлена, як представлено (рис.5):

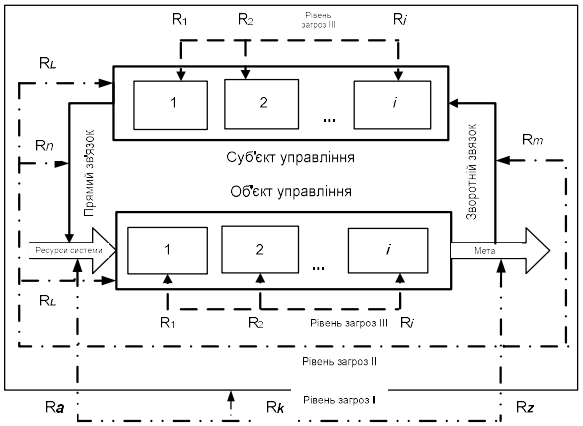


Рис. 5. Модель R-загроз складній системі.

Разом з тим, аналіз ефективності бойового впливу на БПЛА (табл.3) свідчить, що їх бортові системи, особливо такі, що складаються з декількох сенсорів та процесорів, побудовані на контролерах ArduPilotMega (APM) та Pixhawk компаній 3D Robotics, Multiwii, OpenPilot, DJI Naza, є вразливими. Вплив на них дозволяє перехоплювати управління БПЛА, як у режимі дистанційного управління, так й автономно-програмними, за умов незахищеності каналів обміну інформацією.

Для вирішення задачі подолання систем захисту та подальшого впливу на РТС(К) противника необхідно спочатку виявити його у визначеній зоні небезпеки, визначити його місце положення в просторі, розпізнати та розпочати аналіз параметрів, які необхідно оцінити для подальшого комплексного впливу на РТС(К), здійснити комплексний вплив на кіберсистему РТС(К), включно питання формування цілевказівок та команд на фізичне ураження та/або подавлення. Структурно-логічна схема комплексу протиді РТК противника може бути представлена (рис.6)

Будь якому матеріальному об’єкту, у тому числі й БПЛА, притаманні демаскуючі ознаки, які виділяють його серед інших, та надають можливість здійснювати спостереження за ним. Виявлення РТС(К) (БПЛА) може бути здійснено шляхом застосування методів і засособів радіолокації, радіоелектронної розвідки, пасивного акустичного, оптичного та інфрачервоного виявлення в різних діапазонах спектру електромагнітних й звукових хвиль. Оскільки рішення задач виявлення, розпізнавання, супроводження цілей в різних діапазонах спектру базується на різних математичних алгоритмах це суттєво впливає на вирішення єдиної комплексної задачі виявлення, розпізнання та деструктивного впливу на РТС(К).

Рис. 6. Структурно-логічна схема комплексу боротьби з РТС(К) (варіант)

Ступінь спостережності визначається сукупністю характеристик його випромінювань в радіочастотному, акустичному, інфрачервоному (ІЧ) та видимому діапазонах хвиль. Як правило, невеликі БПЛА виготовлені з використанням багатошарових композитних матеріалів, пофарбовані спеціальними фарбами та оснащені бензиновими або електричними двигунами, що виділяють мало тепла та є мало шумними. Вони мають невеликі значення ефективності поверхонь розсіювання (ЕПР) та інтенсивність власного випромінювання [31,32].

Серед способів та методів виявлення та розпізнання БПЛА виділяють:

Акустичний. Виявлення та супроводження БПЛА за акустичними випромінюваннями його механічних складових, насамперед двигуна та гвинта, в бойових умовах вкрай ускладнено, але за окремих умов – можливо, а інколи - доцільно [33, 34].

Оптичний. Оптичне виявлення БПЛА не завжди є ефективним, оскільки значною мірою залежить від природно-кліматичних, просторових та часових факторів, якості оптоелектронного (ОЕ) обладнання та обмежень зони пошуку при використанні вузькосекторних ОЕ засобів. Разом з тим, в комплексі з іншими, більш ефективними засобами виявлення, оптичні та ОЕ засоби можуть ефективно використовуватися для супроводження, наведення на ціль засобів ураження, спостереження за маневрами БПЛА [31,35].

Інфра-червоний. Тепло від двигуна БПЛА, меншою мірою – від електричних та електронних складових та тертя о повітря механічних складових (гвинта, елеронів) може бути джерелом його виявлення. Але, по-перше, потребує спеціального обладнання, по-друге – залежить від багатьох факторів та умов, наприклад таких характеристик БПЛА, як особливості його конструкції щодо зменшення напряму та інтенсивності випромінювання, контрастності фону тощо. ІЧ спосіб виявлення може бути використаний як додатковий, в комплексі з іншими, за певних визначених умов (наприклад, вночі) [31, 35,36].

Радіолокаційний. Спосіб виявлення, розпізнання та супроводження БПЛА, спостереження за його маневрами за допомогою РЛС достатньо ефективний. Забезпечує значну дальність виявлення багатьох цілей. Але - досить енерговитратний, оскільки сучасні БПЛА мають невеликі ЕПР і тому низькі показники коєфіцієнту відбиття радіохвиль. Суттєвим недоліком є висока розвіддоступність та низький рівень захищеності РЛС від ураження противником [31,36,37].

Радіотехнічний. Виявлення, розпізнавання та супроводження БПЛА за випромінюваннями засобів навігації, радіолокації, РЕБ, управління, передачі телеметричної та корисної інформації можливе на значній відстані. Спосіб потребує мінімальних енергозатрат, дозволяє за короткий час встановити пеленг та характеристики руху цілі та забезпечити необхідною інформацією інші засоби виявлення (РЛС, оптичні, ІЧ), а також засоби ураження [31,37].

Аналіз недоліків та переваг зазначених способів виявлення БПЛА дозволяє стверджувати, що для виявлення, розпізнавання та наступного супроводження для здійснення деструктивного впливу на БАК, зокрема на базову платформу-носій (БПЛА), слід застосовувати комплексний підхід.

Комплекси боротьби з наземними, повітряними, надводними та підводними РТС(К) противника повинні забезпечувати виконання таких основних завдань:

1. Визначення найбільш імовірних напрямків, маршрутів руху та тактики дій РТЗ РТС(К) противника.

2. Виявлення, розпізнавання і захоплення на супровід відповідних (наземних, повітряних, надводних або підводних) РТЗ РТС(К) противника у контрольованій зоні за допомогою наявних засобів.

3. Здійснення автоматизованого управління засобами виявлення та протидії РТЗ РТС(К) в режимі часу, близькому до реального.

4. Автоматизоване здійснення обробки та комплексування розвідувальних даних, формування сигнатур об'єктів.

5. Визначення просторових координат РТЗ РТС(К) противника.

6. Визначення засобів та порядку дій щодо протидії РТЗ РТК противника

7. Здійснення видачі цілевказівок засобам протидії.

8. Організація виконання спеціальних заходів боротьби з РТК противника.

Традиційно вважається, що боротьба з РТЗ РТС(К) противника передбачає поетапне вирішення завдань та здійснення процедур їх виявлення (В), захоплення на супроводження та супроводження (С), ідентифікацію (І), видачу цілевказівок та ураження (У) (рис. 7).

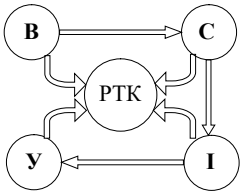


Рис. 7. Існуюча модель ведення боротьби з РТЗ РТС(К) противника

Але застосування традиційних підходів призводить або до несвоєчасного виявлення РТС(К) РТК противника, або ж до неможливості їх ураження за допомогою існуючих засобів.

Крім цього, така модель боротьби має принциповий недолік, який полягає у відсутності можливості запобігання діям РТЗ РТС(К) противника без їх фізичного знищення або знешкодження.

Для усунення зазначених недоліків пропонується розглядати процес боротьби з РТЗ РТК противника як єдину систему, додатковими процедурами якої є прогнозування дій (ПД) РТС(К) та комплексна протидія (КП) ним.

Виявлення факту застосування противником РТЗ РТС(К) є важливим завданням як для

збереження прихованості і раптовості дій військ (сил), так і забезпечення їхньої живучості. Однак застосування існуючих засобів для виявлення сучасних РТЗ РТС(К), які мають малі розміри, виготовляються з композитних матеріалів та можуть діяти в різних умовах обстановки, виявилось проблематичним. З урахуванням зазначеного, підсистема виявлення РТЗ РТС(К) противника повинна являти собою сукупність різнотипних технічних засобів розвідки об'єднаних єдиною системою управління, а запорукою її якісного функціонування є забезпечення принципів формування правил вибору тих засобів, які для заданих умов обстановки забезпечать максимальне значення імовірності правильного виявлення РТЗ РТС(К) противника.

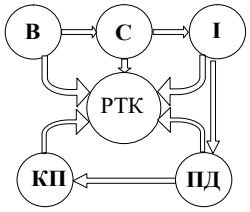


Рис. 8. Перспективна модель ведення боротьби з РТЗ РТС(К) противника

Отже, найбільш дієвим підходом для вирішення завдання виявлення РТЗ РТС(К) противника є застосування комплексних систем, до складу яких можуть входити: комплекси засобів радіолокації (оснащені засобами пасивної радіолокації, засобами активної радіолокації і засобами державної системи радіолокаційного впізнавання); комплекси засобів виявлення супутніх слідів (оснащені ультрафіолетовими приймачами і лазерами); комплекси засобів акустичної розвідки (оснащені засобами виявлення у звуковому діапазоні хвиль і засобами виявлення в ультразвуковому діапазоні хвиль); комплекси засобів оптоелектронної розвідки (оснащені засобами виявлення у видимому діапазоні хвиль, засобами виявлення (ЗВ) в інфрачервоному діапазоні хвиль і засобами виявлення в ультрафіолетовому діапазоні хвиль).

Відповідно до закону кібернетики "необхідної різноманітності", що розкривається, наприклад, в [38], застосування складних систем, якими є робототехнічні системи (комплекси) та системи (комплекси) боротьби з ними (як перші так і другі є в сучасному уявлені кіберфізичними системами), здійснюється керуючими системами, що характеризується різноманітністю цілей застосування, структур, технологій управління тощо. Звідси, на основі [39], моделі РТС(К) і С(К)Б РТС(К), як специфічних КФС можуть бути представлені через зазначені складові та формалізовані таким чином:

$$S \equiv \langle Z, Str, Tech, Cond, Hmn \rangle, \qquad (1)$$

де $Z = \{z_i\}$ – сукупність цілей застосування (функцій РТС(К) і С(К)Б РТС(К));

$Str = \{Str_w, Str_{org}, \ldots\}$ – сукупність засобів, що реалізують цілі застосування (Str_w – виробнича, Str_{org} – організаційна і т.п.);

$Tech = \{meth, means, alg, ...\}$ – сукупність інформаційних технологій (meth – методи, means – засоби, alg – алгоритми і т.п.), що реалізуються системою;

$Cond = \{\varphi_{ex}, \varphi_{in}\}$ – умови існування системи (φ_{ex} - зовнішні, φ_{in} - внутрішні);

Hmn – сукупність показників, що характеризують обслуговуючий персонал (в рамках даного дослідження враховуватися не буде).

При цьому, синтез РТС(К) і С(К)Б РТС(К) передбачає об'єднання складових (1) в єдине ціле відповідно до сукупності цілей застосування.

Сукупністю цілей застосування РТС(К) і С(К)Б РТС(К) є виконання цільових задач за призначенням РТС(К) і протидія цьому С(К)Б РТС(К). Для їх реалізації здійснюється низка узгоджених процесів: інтеграції РТС(К) і С(К)Б РТС(К) до єдиного інформаційно-бойового простору; формування комутаційної матриці вузлів інформаційно-комунікаційної мережі як РТС(К) так і С(К)Б РТС(К); збору відомостей, обробки даних, зберігання інформації в кожній системі (комплексі); управління спеціалізованими базами даних; контролю спроможності виконання складовими РТС(К) і С(К)Б РТС(К) поставлених завдань; оперативних (оперативно-тактичних) розрахунків; забезпечення їх застосування актуальною, достовірною та своєчасною інформацією; інформаційно-аналітичної підтримки прийняття управлінських рішень, що ґрунтується на технологіях моделювання, аналізу ситуацій, прогнозування сценарію їх розвитку тощо; формування сигналів, команд комутації вузлів комунікаційних матриць РТС(К) і С(К)Б РТС(К); захищеного обігу інформації в середині РТЗ РТС(К) та С(К)Б РТС(К).

Далі пропонується об'єднати в загальному для РТС(К) та С(К)Б РТС(К) алгоритмі застосування інформаційні технології моделювання складних динамічних систем, підтримки прийняття рішення, управління тощо.

Так, завдання щодо визначення раціональних структур РТС(К) та С(К)Б РТС(К) може бути сформульоване таким чином: необхідно визначити такий склад підсистем, при якому векторний критерій ефективності

$$Q = \langle I, D, W, O \rangle, \qquad (2)$$

де I – показники інформативності, D – показники ефективності планування застосування сил і засобів РТС(К) та С(К)Б РТС(К) за призначенням,

W – показники ефективності виконання активних дій (кінетичного, некінетичного ураження), O – показники оперативності управління, приймає такі значення, які необхідні для забезпечення максимально ефекту від цільового застосування РТС(К) та С(К)Б РТС(К).

Рішення цієї задачі можливо через реалізацію такого рекурентного алгоритму

$$u = \varphi(A_T, \Theta, UR_\Sigma), \quad u_{N+1} = \varphi(u_N, A_T, \Theta, UR_\Sigma),\ u_{N+1} > u_N. \tag{3}$$

де A_T – потреби, що необхідно задовільними для виконання цільового завдання, $A_T = (a_1, a_2, \cdots, a_i, ..., a_I)$, a_i стан і-ї потреби, що характеризує її сутність;

Θ – вектор показників умов виконання завдань;

UR_Σ наявні засоби, що можуть бути представлені у вигляді об'єднання:

$$UR_\Sigma = \bigcup(UEx, UDs, UAc, SC), \tag{4}$$

де UEx – засоби отримання інформації про об'єкти розвідки, $UEx = \{UEx_1, UEx_2, \ldots, UEx_K\}$;

UDc – засоби управління, $UDc = \{UDc_1, UDc_2, \ldots, UDc_M\}$;

UAc – засоби, які виконують активні дії (кінетичне ураження, радіоелектронне придушення тощо), $UAc = \{UAc_1, UAc_2, \ldots, UAc_N\}$.

Детально алгоритм (3) відносно систем ситуаційного управління розглянуто в [40.].

Декомпозиція алгоритму (3) для РТС(К) і С(К)Б РТС(К) призводить до такої схеми:

1. З'ясування необхідних засобів РТС(К) і С(К)Б РТС(К) для задоволення потреб A_T для виконання цільового завдання

$$I^o_{UR_\Sigma} : \left\{ < UR_i, UC_i > | \, i = \overline{1, M} \right\}, \tag{5}$$

де UR_i – ідентифікатор і-го засобу;

$UC_i = UT_i \bigcup UH_i$ – нормативні спроможності засобів.

2. Оцінювання поточного стану наявних засобів РТС(К) і С(К)Б РТС(К) $I^*_{UR_\Sigma}(t)$, середовища виконання завдань $I_\Theta(t)$,

$$I^*_{UR_\Sigma}(t) = D_{UR}(UR_\Sigma, t), \tag{6}$$

$$I_\Theta(t) = D_\Theta(\Theta, t), \tag{7}$$

де D_{UR}, D_Θ – алгоритми оцінювання.

3. Визначення мети управління Z^* для виконання цільових задач РТС(К) та С(К)Б РТС(К)

$$Z^* = \varphi(A_T, I_\Theta(t), I^*_{UR_\Sigma}(t), I^o_{UR_\Sigma}). \tag{8}$$

У залежності від ситуації метою управління є визначення структури РТС(К) та С(К)Б РТС(К) z_{or} (синтез), її адаптація до змін середовища z_{ad}, реорганізація у разі неможливості задовольнити потреби z_{reorg} поточною структурою, синхронізація діяльності підсистем РТС(К) та С(К)Б РТС(К) z_{cc}, тобто:

$$Z^* = (z_{or}, z_{ad}, z_{org}, z_{cc}). \tag{9}$$

Пошук варіантів (альтернатив) структур РТС(К) та С(К)Б РТС(К) S,

$$S = \left(\bigcup_k UEx_k \bigcup_n UDc_n \bigcup_m UAc_m \right) \bigcap SC, \tag{10}$$

спроможних задовольнити потреби

$$a_i(\Theta, UR) \xrightarrow[u \in U]{} \min. \tag{11}$$

4. Вибір альтернативи з найкращим системним ефектом CA, синтез структури РТС(К) та С(К)Б РТС(К), утворення комунікаційної матриці V^*:

$$CA(A_T, S, \Theta) \to \max. \tag{12}$$

На основі моделі оптимального розподілу ресурсів, що наведена в [41], пропонується така цільова функція забезпечення найбільшого ефекту CA в умовних одиницях від задоволення РТС(К) та С(К)Б РТС(К) потреб:

$$CA = \sum_{i=1}^{n} C_i G_i(t) - \sum_{i=1}^{n} D_i G_i(t) - \sum_{j}^{m} Z_j(1 - G_j(t)) \to \max, \tag{13}$$

$$S_q > \sum_{i=1}^{n} UR_i + \sum_{j=1}^{m} UR_j, \tag{14}$$

де n – кількість потреб, що мають бути задоволені;

C_i – вартість ефекту від задоволення потреби;

m – кількість об'єктів розвідки (впливу) або прикриття;

D_i – витрати на задоволення і-ї потреби;

Z_j – вартість розвідки (впливу) або прикриття j-го об'єкта;

S_q – сумарний ресурс q-ї підсистеми, $q \in \{Ex, Dc, Ac\}$;

UR_i – кількість ресурсів, необхідних для задоволення і-ї потреби (цільової діяльності);

UR_j – кількість ресурсів, необхідних для розвідки (впливу) або збереження j-го об'єкта;

G(t) – індекс функціональної спроможності, сутність та зміст якого розкривається в [42].

На кожному кроці рівень витрат для забезпечення потреб повинен зменшуватися доти, доки не досягне гранично можливого для заданої ефективності виконання завдань та результатів, що очікуються:

$$D_i(A_T, \Theta, UR_\Sigma, u_{N+1}) < D_i(A_T, \Theta, UR_\Sigma, u_N) \tag{15}$$

Тоді, на основі (1) та (13) задача синтезу може бути представлена таким чином:

$$z_{or}: \begin{cases} CA(A_T, S, \Theta) \to \max \\ Q(I, D, W, O) \to extrQ\{\bullet\} \end{cases} \quad (16)$$

Для розв'язання такої багатокритеріальної задачі оптимізації пропонується використовувати метод послідовних поступок [43]. Для цього слід провести ранжирування часткових критеріїв відносно їх важливості у порядку убування O, I, D, W.

Запропонований підхід до синтезу моделей РТС(К) та С(К)Б РТС(К), як КФС, які діють та конфліктують в єдиному інформаційно-бойовому просторі з єдиних позицій, дозволяє в рамках теорій конфліктів та ігр дослідити ефективність застосування як РТС(К) так і С(К)Б РТС(К) в певних умовах, в залежності від їх характеристик, а також визначити вимоги до них.

Висновки й перспективи подальших досліджень

Основоположною тенденцією у воєнній справі на теперішній час та на стратегічну перспективу, є глобальна інформатизація та інтенсивна роботизація військових формувань і створення високоінтегрованих систем управління. Це обумовлено: постійним зростанням можливостей та мініатюризацією комп'ютерних та електронних засобів їх використанням практично в усіх зразках озброєння та бойової техніки (від високоточної до особистої зброї та спорядження), впровадженням засобів штучного інтелекту в системи воєнного призначення, інтеграцією, на основі продуктів високих технологій, систем розвідки, управління та ураження, від підрозділу (одиниці бойової техніки) до командування всіх ланок управління.

РТС(К), в яких інтегровано всі зазначені досягнення в сфері високих технологій, стали невід'ємною складовою сучасної збройної боротьби, що вимагає створення ефективних концепцій, стратегій, форм, способів, методів, тактики і засобів боротьби з ними. Зважаючи, що РТС(К) діють як в природних просторах, так одночасно і в кіберпросторі, і всі вони є, за всіма ознаками, КФС з потужними кіберсистемами управління, то - боротьбу з ними доцільно здійснювати з урахуванням зазначених фактів та на основі пошуку їх кіберфізичних вразливостей і здійснення найбільш раціональних комплексних кібервпливів на них. Проведений аналіз РТС(К) та С(К)Б РТС(К) показав, що зазначений підхід є основоположним при створенні засобів С(К)Б РТС(К), але при цьому і досі відсутні основи теорії і системний підхід до створення С(К)Б РТС(К). В статті надані основоположні підходи до вирішення зазначених питань та запропонований новий підхід до моделювання цих систем, який дозволяє на основі теорій конфліктів та ігор дослідити ефективність застосування як РТС(К) так і С(К)Б РТС(К) в певних умовах, в залежності від їх характеристик, а також визначити вимоги до них.

Література

1. Современные военные роботы: боевые системы будущего [Електронний ресурс] https://militaryarms.ru/voennaya-texnika/boevye-mashiny/voennye-boevye-roboty.

2. В ходе СКШУ "Центр-2015" впервые применена робототехника инженерных войск. [Електронний ресурс]: http://function.mil.ru/news_page/country/more.htm?id=12056386@egNews **3.** "Unmanned Warrior 2016 Technology Fact Sheets", [Електронний ресурс] : https://www.onr.navy.mil/en/Media-Center/unmanned-warrior **4**. Енциклопедія кібернетики: [у 2 т.] / ред.: **В. М. Глушков** (відп. ред) [та ін.]; АН Української РСР. – К. Голов. ред. Укр, рад. енцикл. — 1973. **5**. **Глушков В.М.** (ред.) Словарь по кибернетике. К.: - 1979 **6**. Социологический словарь / отв. ред. **Г.В. Осипов, Л.Н.Москвичев.** М.: - 2014, с. 417. **7.** [Електронний ресурс] https://uk.wikipedia.org/wiki/Безпілотний_літальний_апарат, **8.** Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. – [Електронний ресурс] : http://www.state.gov/secretary/rm/2011/05/163523.htm **9. S.Neema.** Symbiotic Design for Cyber Physical Systems. Defense Advanced Research Projects Agency Program Information **10.** [Електронний ресурс] https://www.darpa.mil/program/symbiotic-design-for-cyber-physical-systems. **11.** [Електронний ресурс]: https://uk.wikipedia.org/wiki/Кіберфізична_система **12.** Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 -Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55. Режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

13. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015. **14. В.Г.Радецький,І.С.Руснак,Ю.Г.Даник** Безпілотна авіація в сучасній збройній боротьбі. Монографія / В.Г.Радецький, І.С.Руснак, Ю.Г.Даник // К.: –2008, НАОУ – 224 с. **15. С.Вдовенко, Ю.Даник**, С.Фараон. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. // Електронний журнал політики відкритого доступу "Комп'ютерні науки та кібербезпека" Харків, ХНУ ім. В.Н.Каразіна – 2019, №1 (12), с.17-29. **16. Ю.Даник, С.Вдовенко** "Ланцюгові ефекти в кібердіях" // Збірник наукових праць ВІКНУ ім. Т. Шевченка - 2019, випуск 64, с. 71-90. **17 Даник Ю.Г., Дупелич С.О.** (2016), Патент UA104494 U. Система виявлення, розпізнавання, супроводження повітряних та наземних цілей. Київ. 4 с. **18. Даник Ю.Г.,Дупелич С.О.**(2016), Патент UA104662 U. Переносний засіб ураження повітряних малорозмірних цілей. Київ.6 с. **19. Ю.Г.Даник, Г.А.Дробаха, В.І.Карпенко** та ін. Теорія і техніка протидії безпілотним засобам повітряного нападу – Х. : ХВУ, 2002. – 260 с. **20. Saravanakumar A.** Exploitation of Acoustic signature of low flying Aircraft using Acoustic

Vector sensor / A. Saravanakumar, K. Senthilkumar // Defence Science Journal. – March 2014. – Vol. 64, No. 2. – P. 95–98. **21.** W. Shi, G.Arabadjis, B.Bishop, P.Hill / Detecting, Tracking and Indentifying Airborne Threats with Netted Sensor Fence // Sensor Fusion – Foundation and Applications. – Rijeka, Croatia : InTech Europe, 2001. – P. 139–158. **22. Ю.Г.Даник.** Основи побудови безпілотних роботизованих систем спеціального призначення : навч. посіб. / Ю.Г.Даник, П.П.Топольницький, І.В.Пулеко та ін. – Житомир: ЖВІ – 2016 – 292 с. **23. Ерёмин Г.В., Гаврилов А.Д., Назарчук И.И.** Организация системы борьбы с малоразмерными БПЛА, Смоленск, ВАВП - 2014 // «Арсенал Отечества» № 6 (14). Режим доступу:https://arsenal-otechestva.ru/article/389-antidrone **24. Р.В.Корольов, Н.О. Королюк, О.В. Петров, К.В. Сюлев.** Аналіз сучасних засобів знищення безпілотних літальних апаратів Харків, ХНУПС – 2017 // Збірник наукових праць Харківського національного університету Повітряних Сил — 2017 — № 4(53). Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/17779 **25.** [Електронний ресурс]: https://fas.org/sgp/crs/weapons/IF11426.pdf; https://lechaim.ru/news/izrailskaya-kompaniya-po-borbe-s-bespilotnikami-predostavit-svoi-sistemy-dlya-fbr-i-amerikanskih-voennyh/; https://defensesystems.com/articles/2019/12/11/counter-uas.aspx; https://russiandrone.ru/news/v_pentagone_vystupili_protiv_dronov_utverdiv_spisok_protivodronnykh_sistem/, https://apps.dtic.mil/dtic/tr/fulltext/u2/1071111.pdf; http://droneflyers.ru/2020/07/13/v-pentagone-vystupili-protiv dronov-utverdiv-spisok-protivodronnyh-sistem-3/; https://www.marketresearch.com/MarketsandMarkets-v3719/Network-Centric-Warfare-Platform-Land-10188278/; http://acronymsandslang.com/definition/24656/BMC4ISR-meaning.html; http://droneflyers.ru/2020/07/13/v-pentagone-vystupili-protiv-dronov-utverdiv-spisok-protivodronnyh-sistem-3/; cyber-physical systems lab. Weapons, Robotics,and Control Engineering; https://www.usna.edu/wrc/cpsl/index.php; https://thebabel.com.ua/news/41889-ssha--ozgortayut-protidronovi-lazerni-sistemi-na-zarubizhnih-bazah; https://lechaim.ru/news/izrailskaya-kompaniya-po-borbe-s-bespilotnikami-predostavit-svoi-sistemy-dlya-fbr-i-amerikanskih-voennyh/; https://www.darpa.mil/program/high-assurance-cyber-military-systems **26.** http://bastion-karpenko.ru/luch-pro-antibla/ ;https://oborona.ru/includes/periodics/defense/2019/0628/123826958/detail.shtml; https://defence-ua.com/index.php/statti/publikatsiji-partneriv/5119-cekretnisystemy-reb-rf-na-donbasi-i-chomu-smm-obsye-dala-yim-14 dniv-fory; http://bastion-karpenko.ru/taran-bla-pro/; http://www.ntc-reb.ru/repelent.html; https://robonews.su/21999-Cheremuha-nahodit-ne-tol-ko-dron-no-i-ego-operatora.html; http://bastion-karpenko.ru/pishal-mfk/; https://www.ao-avtomatika.ru/catalog/products/pishchal-pro/; http:/bastion-karpenko.ru/taran-bla-pro/ ; http:/bastion-karpenko.ru/kupol-pro-antibla/; http:/bastion-karpenko.ru/krasuha-4/ru/kupol-pro-antibla/; http://foto-i-mir.ru/shipovnik-aero/ **27. Вдовенко С.Г. Даник Ю.Г.**, Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління Збройних сил // Сучасні інформаційні технології у сфері безпеки та оборони. К.: - 2017, НУОУ, № 2(29), с. 98-106. **28. В.М.Шлюкін,С.В.Малахов, О.Л. Гостєв, А.Г.Снісаренко, С.Г.Вдовенко, О.М.Присяжний**. Загальносистемні питання санкціонування застосування ракетних комплексів Сухопутних військ // Системи озброєння і військова техніка, Харків – 2012, ХУПС. № 2 (30), с. 95-103. **29. Горбенко І.Д.** Прикладна криптологія. Теорія. Практика. Застосування. монографія / І. Д. Горбенко , Ю. І. Горбенко // Харків. ХНУРЕ, ЗАТ «Ін-т інформ. технологій». – Х. : Форт, 2012. Вид. 2-ге, перероблене й доповнене – 868 с. **30. Вдовенко С.Г. Даник Ю.Г.,** Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення, Зб. мат. Шостої МНТК Методи та засоби кодування, захисту й ущільнення інформації, Вінниця, ВНТУ - 2017, С. 61–64. **31. Даник Ю.В, Бугайов М.В.** Аналіз ефективності виявлення тактичних безпілотних літальних апаратів пасивними та активними засобами спостереження// Збірник наукових праць ЖВІ ДУТ. Інформаційні системи'15. Вип.10. - 2015. – С.5-20. **32. Ю.Г. Даник, І.В.Пулеко, М.В.Бугайов.** Виявлення безпілотних літальних апаратів на основі аналізу акустичних та радіолокаційних сигналів//Вісник ЖДТУ - 2014, № 4 (71). С.71-80. **33. В.М.Олейніков, О.В.Зубков, В.М.Карташов, І.В. Корытцев, С.І.Бабкин, С.О.Шейко**. Исследование эффективности обнаружения и распознавания малоразмерных беспилотных летательных аппаратов по их акустическому излучению Радиотехника. 2018 Вип. 195. Режим досупу: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_195_23.pdf **34. В.М.Карташов, В.М.Олейніков, С.О.Шейко, С.І.Бабкин, І.В. Корытцев, О.В.Зубков** Особенности обнаружения и распознавания малых беспилотных летательных аппаратов Радиотехника. 2018. Вип. 195: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_195_26.pdf **35. Соловьев В. А.** Проблемы обнаружения беспилотных летательных аппаратов оптико-электронными устройствами / В. А. Соловьев // Электронный математический и медико-биологический журнал. – Т. 10, 2011. – Вып. 3. – С. 1–13. **36. Moses A.** Radar-based detection and identification for miniature air vehicles / A. Moses, M. J. Rutherford, K. P. Valavanis // IEEE International Conference on Control Applications **37. Zelnio A.M.** Detection of small aircraft using an acoustic array. Thesis. B.S. / A.M. Zelnio. – Electrical Engineering, Wright State University. - 2007. – 55 p. **38. Пьявченко Т.А., Финаев В.И.** Автоматизированные информационно-управляющие системы. Таганрог: Изд-во ТРТУ, 2007. 271 с. **39. Згуровський М.З., Панкратова Н.Д.** Основи системного аналізу: підручник. Київ: Видавнича група ВНУ, 2007. 544 с. **40. Даник Ю.Г, Шестаков В.І.** Методологія синтезу ситуаційних розвідувально-ударних комплексів. Сучасні інформаційні технології у сфері безпеки та оборони, 2019. №2(35). С. 13–22. **41. Литвак Б.Г.** Разработка управленческого решения. Изд. 3-е., испр. Москва: Дело, 2002. 392 с. **42. Даник Ю.Г, Шестаков В.І.** Методологія синтезу ситуаційних розвідувально-ударних комплексів. Сучасні інформаційні технології у сфері безпеки та оборони, 2019. №2(35). С. 13–22. **43. Воронин А.Н., Зиатдинов Ю.К., Кукпинский М.В.** Многокритериальные решения: модели и методы: монография. Киев: НАУ, 2011. 348 с.

КИБЕРПРОТВОДЕЙСТВИЕ РОБОТОТЕХНЧЕСКИМ КОМПЛЕКСАМ

Сергей Григорьевич Вдовенко
Юрий Григорьевич Даник *(доктор технических наук, профессор)*
Александр Юрьевич Пермяков *(доктор технических наук, профессор)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Стремительное развитие, массовое производство, принятие на вооружение и растущее число фактов боевого применения в военных конфликтах современности высокотехнологичных систем вооружения и робототехнических систем (комплексов) (РТС(К)) требуют осуществления мероприятий по созданию эффективной системы противодействия РТК. В частности, разработки стратегий и концепций, теории и тактики противодействия РТК, переосмысление канонов оперативного искусства и тактики применения существующих средств ПВО в контексте борьбы с РТС(К), предъявления требований по модернизации и развитию систем (комплексов) борьбы с РТС(К) (С(К)БРТС(К)), проведения научных исследований, научно-исследовательских и опытно-конструкторских работ по созданию средств и систем (комплексов) противодействия РТС(К), организации подготовки квалифицированных специалистов по их эксплуатации и боевому применению, научно-педагогических кадров и т.д. Учитывая, что по своим признакам РТС(К) являются киберфизическими системами (КФС) специального назначения, а их системы управления - классическими кибернетическими системами, приоритетными являются подходы по созданию единых принципов борьбы с РТС(К) (тех типов и классов, с которыми невозможно или неэффективно бороться существующими средствами) и систем для их реализации, состоящих из органов управления и подразделений, имеющих на вооружении системы (комплексы) ВВТ со специфическими программно-аппаратными средствами и комплексы для решения указанных задач.

В статье представлены результаты: анализ эффективности применения существующих систем вооружения для борьбы с БПЛА поля боя беспилотных авиационных комплексов (БАК); анализ уязвимости составляющих РТС(К); анализ тенденций развития систем (комплексов) борьбы с РТС(К) (БПЛА БАК) ведущих государств в контексте возможности и целесообразности внедрения их опыта в Украине; представление основных теоретических положений формирования систем киберпротиводействия РТС(К) как КФС.

Ключевые слова: *беспилотные авиационные комплексы (БАК), беспилотные летательные аппараты (БПЛА), боевое применение робототехнических систем (комплексов), выявление робототехнических комплексов (средств), киберсистемы, киберфизические системы (КФС), робототехнические системы (комплексы) (РТС(К)), системы (комплексы) борьбы с робототехническими системами (комплексами) С (К) Б РТС (К)).*

CYBER COUNTERACTION TO ROBOTIC COMPLEXES

Serhii Vdovenko
Yurii Danyk *(**Doctor of Technical Science, Professor)***
Oleksandr Permiakov *(**Doctor of technical sciences, Professor)***

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The rapid development, mass production, adoption and the growing number of facts of combat use in hostilities and conflicts of modern high-tech weapons systems and robotic systems (complexes) require a number of measures to create an effective system to counter them.

In particular, the development of strategies and concepts, theories and tactics of countering robotic technical complexes, rethinking the canons of operational art and tactics of existing air defense in the context of combating robotic technical complexes, developing requirements for modernization and development of systems (complexes) to combat them, research, research and development work on the creation of means and systems (complexes) of counteraction to robotic complexes, organization of training of qualified specialists in their operation and combat use, scientific and pedagogical staff, etc.

Given that robotic systems are special-purpose cyber physical systems and their control systems are classical cybernetic systems, priority is given to approaches to creating a single framework for combating robotic systems (those types and classes that cannot or ineffectively deal with existing means) and systems for their implementation, consisting of management bodies and appropriately equipped units, which are armed with systems (complexes) of armaments and military equipment with specific software and hardware and complexes to solve these problems.

The article presents the results: analysis of the effectiveness of the use of existing weapons systems to combat small unmanned aerial vehicles of unmanned aerial complexes; vulnerability analysis of components of robotic complexes; analysis of development trends in the world's leading countries of systems (complexes) to combat robotic systems (for example, unmanned aerial vehicles of unmanned aerial complexes) in the context of the possibility and feasibility of implementing their experience in Ukraine; development of basic theoretical provisions for the formation of cyber counteraction systems for robotic technical complexes as cyber physical systems

Keywords: *cyber systems, cyber physical systems, combat use of robotic systems (complexes), detection of robotic complexes (means), systems (complexes) counter, combat robotic systems, unmanned aerial complex, unmanned aerial vehicle.*

References

1. Modern soldiery robots are the battle systems of the future [Sovremennyie voennyie robotyi – boevyie sistemyi buduschego], available at: https://militaryarms.ru/voennaya-texnika/boevye-mashiny/voennye-boevye-roboty. **2**. During manoeuvres "Center-2015" robotics of engineering troops is first used [V hode SKShU «Tsentr-2015» vpervyie primenyaetsya robototehnika inzhenernyih voysk], Access mode:://function.mil.ru/news_page/country/more.htm?id=12056386@egNews **3.** Unmanned Warrior 2016 / Technology Fact Sheets", Access mode:https://www.onr.navy.mil/en/Media-Center/unmanned-warrior **4**. Entsiklopediia kibernetiky [Encyclopedia of Cybernetics] (1973) [in 2 volumes] / ed .: **VM Glushkov** (ed.) [Etc.]; Academy of Sciences of the Ukrainian SSR. - K. Golov. ed. Ukr, rad. encyclical. **5**. **Glushkov VM** (ed.) (1979) / Slovar po kybernetyke [Dictionary of Cybernetics]. **6**. Sotsyolohycheskyi slovar (2014) [Sociological dictionary] / resp. ed. **G.V.Osipov, LN.Moskvichev**. p.417. **7.** Access mode: https://uk.wikipedia.org/wiki/Безпілотний_літальний_апарат, **8.** Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. – Access mode:http://www.state.gov/secretary/rm/2011/05/163523.htm **9. S.Neema.** Symbiotic Design for Cyber Physical Systems. Defense Advanced Research Projects Agency Program Information **10.** Access mode: https://www.darpa.mil/program/symbiotic-design-for-cyber-physical-systems. **11.** available at: https://uk.wikipedia.org/wiki/Кіберфізична_система **12.** Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 -Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55. Access mode:: https://www.nato.int/cps/en/natohq/official_texts_133169.htm **13.** Stratehiia natsionalnoi bezpeky Ukrainy / [National Security Strategy of Ukraine], approved by the Decree of the President of Ukraine dated 26.05.2015 № 287/2015. **14. VG Radetsky, IS Rusnak, YG Danyk**. (2008) Bezpilotna aviatsiia v suchasnii zbroinii borotbi. [Unmanned aerial vehicles in modern armed struggle]. Monograph / VG Radetsky, IS Rusnak, YG Danyk // 224 p. **15. S. Vdovenko, Y. Danik, S. Faraon**. (2019). Definitsiini problemy terminolohii u sferi kiberbezpeky i kiberoborony ta shliakhy yikh vyrishennia. [Definitive problems of terminology in the field of cybersecurity and cyber defense and ways to solve them.] // Electronic Journal of Open Access Policy "Computer Science and Cybersecurity" Kharkiv, KhNU. VNKarazin, №1 (12), p.17-29. **16. Yu. Danyk, S. Vdovenko** (2019) Lantsiuhovi efekty v kiberdiiakh. [Chain effects in cyber actions.] // Collection of scientific works of the WINDOW named after T. Shevchenko, issue 64, p. 71-90. **17. Danyk Yu. H.,** Dupelych S. O. (2016), Patent of UA104494 U. Systema vyiavlennia, rozpiznavannia, suprovodzhennia povitrianykh ta nazemnykh tsilei. [System of exposure, recognition, accompaniment of air and surface aims.], Kyiv, 6 p. **18. Danyk Yu.G., Dupelych S.O.** (2016), Patent of UA104662 U. Perenosnyi zasib urazhennia povitrianykh malorozmirnykh tsilei [Portable decimator of air littlesize aims.], Kyiv, 4 p.**19. YG Danyk, GA Drobakha, VI Karpenko** and others. (2002). . Teopiia i tekhnika protydii bezpilotnym zasobam povitrianoho napadu. [Theory and technique of counteracting unmanned aerial vehicles], Kharkiv - 260 p.**20. Saravanakumar A.** Exploitation of Acoustic signature of low flying Aircraft using Acoustic Vector sensor / A. Saravanakumar, K. Senthilkumar // Defence Science Journal. – March 2014. – Vol. 64, No. 2. – P. 95–98. **21. W.Shi, G.Arabadjis, B.Bishop, P.Hill** (2001) / Detecting, Tracking and Indentifying Airborne Threats with Netted Sensor Fence // Sensor Fusion – Foundation and Applications. – Rijeka, Croatia : InTech Europe, – P. 139–158. **22. YG Danyk PP Topolnytsky, IV Puleko** and others (2016). Osnovy pobudovy bezpilotnykh robotyzovanykh system spetsialnoho pryznachennia. [Fundamentals of construction of unmanned robotic systems for special purposes:] / textbook / Zhytomyr — 292 p. **23. Eremin GV, Gavrilov AD, Nazarchuk II.** Orhanyzatsyia sistemy borby s malorazmernymi BPLA [Organization of the system of control of small UAVs] (2014), Smolensk, // Arsenal of the Fatherland, № 6 (14). Access mode: https://arsenal-otechestva.ru/article/389-antidrone/ **24. RV Korolov, NO Koroliuk, OV Petrov, KV Sulev**. (2017). Analiz suchasnykh zasobiv znyshchennia bezpilotnykh litalnykh aparativ. [Analysis of modern means of destruction of unmanned aerial vehicles] / Kharkiv // Collection of scientific works of Kharkiv National University of the Air Force № 4 (53). Access mode: http://www.hups.mil.gov.ua/periodic app / article / 17779 **25.** Access mode:: https://fas.org/sgp/crs/weapons/IF11426.pdf; https://lechaim.ru/news/izrailskaya-kompaniya-po-borbe-s-bespilotnikami-predostavit-svoi-sistemy-dlya-fbr-i-amerikanskih-voennyh/; https://defensesystems.com/articles/2019/12/11/counter-uas.aspx; https://russiandrone.ru/news/v_pentagone_vystupili_protiv_dronov_utverdiv_spisok_protivodronnykh_sistem/, https://apps.dtic.mil/dtic/tr/fulltext/u2/1071111.pdf; http://droneflyers.ru/2020/07/13/v-pentagone-vystupili-protiv dronov-utverdiv-spisok-protivodronnyh-sistem-3/; https://www.marketresearch.com/MarketsandMarkets-v3719/Network-Centric-Warfare-Platform-Land-10188278/; http://acronymsandslang.com/definition/24656/BMC4ISR-meaning.html; http://droneflyers.ru/2020/07/13/v-pentagone-vystupili-protiv-dronov-utverdiv-spisok-protivodronnyh-sistem-3/; cyber-physical systems lab. Weapons, Robotics,and Control Engineering; https://www.usna.edu/wrc/cpsl/index.php; https://thebabel.com.ua/news/41889-ssha--ozgortayut-protidronovi-lazerni-sistemi-na-zarubizhnih-baza h; https://lechaim.ru/news/izrailskaya-kompaniya-po-borbe-s-bespilotnikami-predostavit-svoi-sistemy-dlya-fbr-i-amerikanskih-voennyh/; https://www.darpa.mil/program/high-assurance-cyber-military-systems **26.** Access mode:: http://bastion-karpenko.ru/luch-pro-antibla/ ;https://oborona.ru/includes/periodics/defense/2019/0628/123826958/detail.shtml; https://defence-ua.com/index.php/statti/publikatsiji-partneriv/5119-cekretnisystemy-reb-rf-na-donbasi-i-chomu-smm-obsye-dala-yim-14 dniv-fory; http://bastion-karpenko.ru/taran-bla-pro/; http://www.ntc-reb.ru/repelent.html; https://robonews.su/21999-Cheremuha-nahodit-ne-tol-ko-dron-no-i-ego-operatora.html; http://bastion-karpenko.ru/pishal-mfk/; https://www.ao-avtomatika.ru/catalog/products/pishchal-pro/; http://bastion-karpenko.ru/taran-bla-pro/ ;-http://bastion-karpenko.ru/kupol-pro-antibla/; http://bastion karpenko.ru/krasuha-4/ru/kupol-pro-antibla/; h tp://foto-i-mir.ru/shipovnik-aero/ **27. Vdovenko SG Danyk Yu.G**., (2017). Kontseptualni napriamy kompleksnoho vyrishennia problemy zakhystu informatsii v systemi skrytoho upravlinnia Zbroinykh syl. [Conceptual directions of complex solution of the problem of information protection in the system of covert management of the Armed Forces] // Modern information technologies in the field of security and

defense. Kyiv, № 2 (29), c. 98 106. **28. VM Shlyukin, SV Malakhov, OL Gostev, AG Snisarenko, SG Vdovenko, OM Prysyazhny.** (2012). Zahalnosystemni pytannia sanktsionuvannia zastosuvannia raketnykh kompleksiv Sukhoputnykh viisk [General system issues of authorizing the use of missile systems of the Land Forces] // Weapons Systems and Military Equipment, Kharkiv. № 2 (30), p. 95-103. **29. ID Gorbenko** (2012). Prykladna kryptolohiia. Teoriia. Praktyka. Zastosuvannia. [Applied cryptology. Theory. Practice. Application.] Monograph / ID Gorbenko, YuI Gorbenko // Kharkiv, CJSC "Inst of Inform. technologies ". Fort. Kind. 2nd, revised and supplemented - 868 p. **30. SG Vdovenko Yu.G Danik.** (2017). Kontseptualni napriamky kompleksnoho vyrishennia problemy zakhystu vid nesanktsionovanoho dostupu v skladnykh systemakh spetsialnoho pryznachennia. [Conceptual directions of the complex decision of a problem of protection against unauthorized access in difficult systems of special purpose] // Collection of materials of the Sixth ISTC Kontseptualni napriamky kompleksnoho vyrishennia problemy zakhystu vid nesanktsionovanoho dostupu v skladnykh systemakh spetsialnoho pryznachennia [Methods and means of coding, protection and consolidation of the information], Vinnytsia,, P. 61–64. **31. Danik Yu.V., Bugayov MV** (2015) Analiz efektyvnosti vyiavlennia taktychnykh bezpilotnykh litalnykh aparativ pasyvnymy ta aktyvnymy zasobamy sposterezhennia [Analysis of the effectiveness of detection of tactical unmanned aerial vehicles by passive and active means of surveillance] // Zhytomyr. Collection of scientific works of ZhVI DUT. Information Systems'15. Issue 10. - P.5-20. **32. Yu.G. Danyk, IV Puleko, MV Bugayov** (2014) Vyiavlennia bezpilotnykh litalnykh aparativ na osnovi analizu akustychnykh ta radiolokatsiinykh syhnaliv [Detection of unmanned aerial vehicles based on the analysis of acoustic and radar signals.] / Zhytomyr. Bulletin of ZhSTU, № 4 (71). P.71-80.**33. VM Oleynikov, OV Zubkov, VM Kartashov, IV Korytsev, SI Babkin, SO Sheiko** (2018). Issledovaniye effektivnosti obnaruzheniya i raspoznavaniya malorazmernykh bespilotnykh letatelnykh apparatov po ikh akusticheskomu izlucheniyu [Research of efficiency of detection and recognition of small-sized unmanned aerial vehicles on their acoustic radiation.] // Radio engineering. Vol. 195. Access mode: https://nure.ua/wp content / uploads / 2018 / Scientific_editions / rvmnts_2018_195_23.pdf **34. VM Kartashov, VM Oleynikov, SO Sheiko, SI Babkin, IV Korytsev, OV Zubkov** (2018). Osobennosti obnaruzheniya i raspoznavaniya malykh bespilotnykh letatelnykh apparatov [Features of detection and recognition of small unmanned aerial vehicles] / Radio engineering. Vol. 195. Access mode:: https://nure.ua/wp-content/uploads/ 2018/Scientific_editions / rvmnts_2018_195_26.pdf **35. Soloviev VA** (2011). Problemy obnaruzheniya bespilotnykh letatelnykh apparatov optiko-elektronnymi ustroystvami [Problems of detection of unmanned aerial vehicles by optoelectronic devices] / VA Soloviev // Electronic mathematical and medical-biological journal. - Vol. 10. Issue. 3. - P. 1–13. **36. Moses A**. Radar-based detection and identification for miniature air vehicles / A. Moses, M. J. Rutherford, K. P. Valavanis // IEEE International Conference on Control Applications **37. Zelnio A.M.** Detection of small aircraft using an acoustic array. Thesis. B.S. / A.M. Zelnio. – Electrical Engineering, Wright State University. - 2007. – 55 p. **38. Pyavchenko TA, Finaev VI** (2007) Avtomatizirovannyye informatsionno-upravlyayushchiye sistemy. [Automated information and control systems] Taganpog: TRTU Publishing House. 271 p. **39. Zgurovsky MZ, Pankratova ND** (2007). Osnovy systemnoho analizu / [Fundamentals of systems analysis]: a textbook. Kyiv: University Publishing Group, 2007. 544 p. **40. Danyk Yu.G., Shestakov** VI (2019) / Metodolohiia syntezu sytuatsiinykh rozviduvalno-udarnykh kompleksiv. [Methodology of synthesis of situational reconnaissance and strike complexes.] / Modern information technologies in the field of security and defense. №2 (35). Pp. 13–22.**41. Litvak BG** Razrabotka upravlencheskogo resheniya. [Development of a management decision.] (2002). Ed. 3rd, corrected. Moscow: Delo, 392 p.**42. Danyk Yu.G., Shestakov VI** (2019) Metodolohiia syntezu sytuatsiinykh rozviduvalno-udarnykh kompleksiv. [Methodology of synthesis of situational reconnaissance and strike complexes] / Modern information technologies in the field of security and defense. №2 (35). Pp. 13–22. **43.Voronin AN, Ziatdinov Yu. K., Kukpinsky MV** (2011). Mnogokriterialnyye resheniya: modeli i metody/[Multicriteria solutions: models and methods]: monograph. Kyiv: NAU ,. p. 348.