ҒТАХР 55.47.07
https://doi.org/10.56132/2791-3368-2026-1-65-17-27

Г.Б. Кашаганова [1], Д.Ж. Сатыбалдина [2], М. Жасандықызы[3]
[1]Satbayev University, Алматы, Қазақстан
[2]L.N. Gumilyov Eurasian National University, Алматы, Қазақстан
[3]International Information Technology University, Алматы, Қазақстан
E-mail: guljan_k70@mail.ru

ҰШҚЫШСЫЗ ҰШУ АППАРАТТАРЫНЫҢ КИБЕРҚАУІПСІЗДІК ҚАТЕРЛЕРІН ЗЕРТТЕУ

Аңдатпа. Соңғы он жылда ұшқышсыз ұшу аппараттарын (ҰҰА) зерттеу олардың бірегей қасиеттері мен әскери саласында, ауыл шаруашылығында, мониторингте, бақылауда, бейне-фототүсірілім кезінде және басқа салаларда көптеген пайдалану жағдайларына байланысты айтарлықтай кеңейді. Кеңінен қолданылғанына қарамастан, ҰҰА киберқауіпсіздіктің маңызды мәселелеріне тап болады. ҰҰА әртүрлі кибершабуылдарға осал, өйткені олар кибернетикалық және физикалық компоненттер бір-бірімен тығыз байланысты күрделі жүйелер. Шабуылдаушылар осы компоненттерге, олардың арасындағы интерфейстерге, сымсыз байланыс арналарына немесе екеуінің тіркесіміне шабуыл жасай алады. ҰҰА негізгі киберқауіптері – шабуылдаушыларға құрылғыны басқаруға мүмкіндік беретін рұқсатсыз қол жеткізу және бақылауды алу, жиналған деректерді ұрлау немесе ағызу, сондай-ақ деректерді бұрмалау (алдау). Деректерді қорғау үшін шифрлау жүйелері, түпнұсқалықты растау үшін аутентификация механизмдері, ауытқуларды анықтау үшін киберқауіптерді талдау және болжау алгоритмдері сияқты сенімді қорғаныс шараларын әзірлеу сұрақтары осы мақалада қарастырылған.

Түйінді сөздер: ұшқышсыз ұшу аппараты, киберқауіпсіздік, кибершабуылдар, қорғау шаралары.

Кіріспе.

Дрондар деп аталатын ұшқышсыз ұшу аппараттары (ҰҰА) автономды немесе қашықтан басқарылатын күрделі техникалық жүйелер болып табылады. Олар белгілі бір кеңістіктік және уақыттық шекараларда бағдарламаланған маршруттар бойынша қозғалыс орындай алады. Аппараттық және бағдарламалық жасақтама компоненттерін біріктіре отырып, дрондар деректерді жинауды, өңдеуді және беруді жүзеге асырады, бұл кибершабуылдарға ықтимал осалдықтар тудырады. Дрондар әскери және азаматтық міндеттердің кең спектрінде, соның ішінде барлау операцияларында, аумақтарды бақылауда, ғылыми ізденістерде, іздеу жұмыстарында, инфрақұрылымды басқаруда және көлік тасымалында

қолданылады. Бастапқыда олар әскери мақсатта дамыды, уақыт өте келе олар әртүрлі қосымшалар үшін маңызды құралға айналды, соның ішінде ауыл шаруашылығы [1] және информатика, робототехника, жасанды интеллект, фотограмметрия және қашықтықтан зондтау сияқты ғылыми салалар [2].

ҰҰА мобильді сымсыз желілерде ұшатын базалық станциялар ретінде әрекет ете алады және клиенттердің шектеулеріне немесе құнына байланысты стационарлық ұялы станцияларды салу мүмкін емес жерлерде телекоммуникациялық қызметтерді ұсына алады [3]. Сонымен қатар, ҰҰА төтенше жағдайларды жою операцияларында, ауа-райын бақылауда, өнеркәсіптік инфрақұрылымды бақылауда, логистикалық көмек көрсетуде, зардап шеккен аймақтардағы апаттарды жылдам басқаруда және үйлерді бақылауда маңызды рөл атқарады [4].

Әр түрлі салаларда ҰҰА пайдалану қауіпсіздікке қауіп төндіреді, өйткені бұл жүйелер зиянкестер үшін ерекше қызығушылық тудырады. Атап айтқанда, жердегі басқару станцияларының осалдығы деректерді ұрлауды және зиянды командаларды енгізуді қоса алғанда, кибершабуылдарды жүзеге асыруға мүмкіндік береді.

Бұл мақалада ҰҰА киберқауіпсіздігінің өзекті мәселелері жан-жақты зерттеледі, олар архитектурасы мен функционалдық сипаттамаларының ерекшеліктеріне байланысты пайдаланудың барлық кезеңдерінде - деректерді жинау мен өңдеуден бастап ұшуды басқаруға дейінгі зиянкестер үшін осал нысанаға айналады. Нақты уақыттағы шабуылдарды анықтау үшін шифрлау, көп факторлы аутентификация және қауіп-қатерді талдау алгоритмдері сияқты заманауи қорғаныс әдістеріне ерекше назар аударылады.

Материалдар мен әдістер.

Ұшқышсыз ұшу аппараттары.

ҰҰА аэродинамикалық күштер есебінен оларды ауаға көтеретін қозғалтқыштармен жарақтандырылған, арнайы берілген траектория бойынша дербес режимде жұмыс істейтін немесе қашықтықтан операторлармен басқарылатын, арнайы техникалық құралдарымен, бейне және фотофиксация аппаратурасымен, өзге де барлау және барлау аппаратурасымен қосымша жарақтандыру үшін әлеуеті бар экипажсыз бірнеше рет пайдаланылатын аппараттар ретінде айқындауға болады жер беті мен су ортасын бақылау. Әр түрлі мүмкіндіктер, жоғары техникалық сипаттамалар және осы құрылғылардың тез таралуы оларды өмірдің әртүрлі салаларында қолдану үшін барынша сұранысқа ие етеді.

ҰҰА жіктелуі келесідей:

– Басқару әдісі бойынша – қашықтықтан және автоматты;

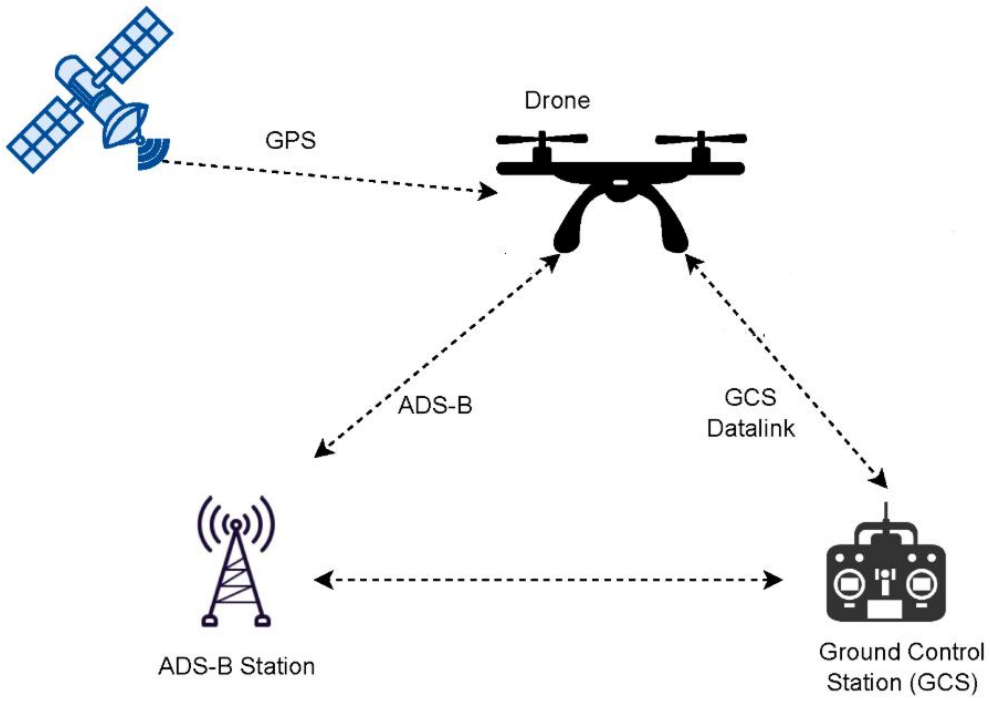
– Басқару түрі бойынша – айналмалы және бекітілген қанат;

– Салмағы және көлемі бойынша – микро мини, тактикалық, стратегиялық және арнайы мақсаттағы;

– Қолданылуы бойынша – тасымалдау, бейне және фото түсірілімдер, әскери сала.

Дрондарды жіктеу келесі параметрлер бойынша жүзеге асырылады: мөлшері, ұшу жылдамдығы, пішіні, максималды көтерілу биіктігі және ұшу ұзақтығы. ҰҰА басқару алдын ала орнатылған бағдарламалық құрал немесе алгоритмдер арқылы жүзеге асырылады және навигация GPS, инерциялық өлшеу жүйелері, компастар және басқа датчиктер арқылы қамтамасыз етіледі. Бұл жүйелер максималды жылдамдық, диапазон, жұмыс уақыты, жүк көтергіштігі, камера мен датчиктердің сапасы сияқты дрондардың техникалық сипаттамаларын анықтайды.

Ұшқышсыз жүйелердің негізі: жердегі контроллер, датчиктер, жетектер, қуатты басқару жүйесі, ұшуды басқару тақтасы, айналмалы жүйе, жылдамдық реттегіші және радиобайланысты басқару блогы. 1-суретте ҰҰА құрылымдық сұлбасы көрсетілген.



1 сурет – ҰҰА құрылымдық сұлбасы

Ұшқышсыз жүйелердің архитектурасында үш негізгі компонентті ажыратуға болады: ҰҰА, жердегі басқару станциясы және деректер арналары. Дронның дизайны энергетикалық жүйені, борттық басқару компьютерін, дәл навигациялық ішкі жүйені және өлшеу датчиктерінің жиынтығын қамтиды.

ҰҰА - ұшатын робот сияқты жұмыс істейтін жүйенің орталық мобильді құрамдас бөлігі, оны қашықтан немесе офлайн режимде бағдарламалық түрде берілген ұшу жоспарларын пайдалана отырып басқаруға болады.

ҰҰА төрт негізгі түрі бар: әртүрлі конфигурацияларда бірнеше қозғалтқыштармен жабдықталған көп роторлы дрондар (үш роторлы трикоптерлер, төрт роторлы квадрокоптерлер, алтауы бар гексакоптерлер және сегізі бар октокоптерлер); ұшақ принципі бойынша жұмыс істейтін

және ауада позицияны тұрақты ұстаудың қажеті жоқ энергия тиімділігімен ерекшеленетін бекітілген қанатты дрондар; бір роторлы дрондар жалғыз тірек бұрандасы; сонымен қатар көп роторлы және бекітілген қанатты жүйелердің артықшылықтарын біріктіретін гибридті тік ұшу және қону машиналары. 2- суретте ҰҰА түрлері көрсетілген.

2 сурет 2– ҰҰА түрлері

ҰҰА маңызды құрамдас бөлігі – датчиктерден деректерді жинайтын, оларды басқару сигналдарына түрлендіретін және жұмыс режиміне байланысты ақпаратты жердегі басқару жүйесіне (ЖБЖ) жіберетін немесе ҰҰА мен ЖБЖ арасындағы байланыс интерфейсін қамтамасыз ете отырып, жетектердің жұмысын тікелей реттейтін ұшу контроллері.

Жердегі басқару жүйесі ҰҰА жедел басқарудың және миссияның барлық кезеңдерінде олардың жұмысын бақылаудың негізгі платформасы ретінде қызмет етеді, басқару командаларын беру және нақты уақыттағы телеметриялық деректерді қабылдау үшін тұрақты сымсыз байланысты қамтамасыз етеді, ЖБЖ масштабы мен конфигурациясы пайдаланылатын ұшқышсыз ұшу аппараттарының түріне және шешілетін тапсырмалардың ерекшеліктеріне байланысты өзгереді тактикалық және стратегиялық міндеттерді шешуге арналған көптеген жұмыс орындары бар орналастырылған стационарлық кешендерге арналған портативті пульттер.

Деректерді беру арнасы басқару сигналдары мен телеметриялық ақпарат алмасуды қамтамасыз ететін ҰҰА мен ЖБЖ арасындағы сымсыз байланыс болып табылады, бұл ретте байланыстың нақты түрін таңдау аппараттың қажетті әрекет ету радиусымен анықталады. ҰҰА пайдалану оператор мен дрон арасындағы радиоарна арқылы басқарылатын тікелей көріну режимінде немесе спутниктік жүйелер немесе басқа дрондарды қоса алғанда, қайталағыш желі арқылы байланыс сақталатын көріну аймағынан тыс режимде жүзеге асырылады, бұл бақылау аймағын жаһандық ауқымға дейін кеңейтуге мүмкіндік береді.

ҰҰА перспективалық құрылымдар бірқатар негізгі талаптарға сәйкес келуі керек: қарапайымдылық, жеңіл салмақ, әртүрлі қолдану сценарийлеріне бейімделу үшін модульділік, сондай-ақ экономикалық тиімділік және күрделі рельефке және су бетіне қауіпсіз қону мүмкіндігі.

Функционалдылықты кеңейту үшін жасанды интеллектке негізделген өзін-өзі қалпына келтіру жүйесі және борттық 3D басып шығару сияқты

инновациялық шешімдерді енгізуге болады. Платформа датчиктер мен энергия көздерінің әртүрлі түрлерін біріктіруге мүмкіндік беруі керек. Сондай-ақ, ұшудың әртүрлі кезеңдерінде ұшу сипаттамаларын оңтайландыруға мүмкіндік беретін өзгермелі геометрия қанатын қолдану дамудың маңызды бағыты болып табылады. Бұл технология тапсырмаға байланысты жылдамдық пен жүктеме қатынасының икемді таңдауын қамтамасыз етеді.

ҰҰА оларды анықтау және қарсы тұру міндетін қиындататын негізгі артықшылықтары:

– операторды қауіпсіз жою кезінде тапсырмаларды қашықтан орындау мүмкіндігі және сонымен бірге операторды нақты уақыт шкаласында орындалатын тапсырманың барысы туралы ақпаратпен қамтамасыз ету;

– қазіргі заманғы элементтік базада шағын габаритті нысаналы жүктемелердің кең спектрін, радиоэлектрондық барлау құралдарын, жауынгерлік бөлімдерді қолдану;

– басқарылатын ұшу аппараттарымен салыстырғанда төмен массалық габариттік сипаттамаларға және ұшқышсыз ұшу аппараттарының конструкциясында пластикалық және композиттік материалдарды кеңінен қолдануға байланысты радиолокациялық және оптикалық диапазондарда ұшқышсыз ұшу аппараттарының төмен байқалуы;

– жоғары жүктемелермен маневрлер жасау және әуе шабуылына қарсы қорғаныстың қолданыстағы және перспективалы құралдарының тиімділігінің төмендеуіне әкелетін ұшу режимін пайдалану мүмкіндігі – жер бедерінің қорғаныш қасиеттерін пайдалана отырып, өте төмен биіктікте (50 м дейін), сондай-ақ төмен ұшу жылдамдығында (10-30 м/с)ұшу мүмкіндігі;

– шағын геометриялық өлшемдер;

– олардың қозғалтқыштарының салыстырмалы үнсіздігімен қамтамасыз етілетін ұшқышсыз ұшу аппараттарын қолданудың құпиялылығы;

– тұрақтылық пен басқарудың қарапайымдылығын қамтамасыз ететін классикалық аэродинамикалық сұлбаны қолдану;

– ҰҰА пайдаланудың қарапайымдылығымен ерекшеленетін электр қозғалтқыштарымен жарақтандыру мүмкіндігі;

– қозғалтқыштар үшін (күн батареялары, криогендік отын) дәстүрлі емес энергия түрлерін пайдалану мүмкіндігі, олардың ұшу уақытын шектемей ұшқышсыз ұшу аппараттарын қолдануға мүмкіндік береді.

ҰҰА тиімділігін арттыруды тапсырманы нақты бөлу шартымен шағын арзан ұшқышсыз ұшу аппараттарын топтарға біріктіру арқылы жүзеге асыруға болады.

ҰҰА негізгі кемшіліктері.

– ҰҰА жекелеген санаттары үшін тәулік уақытына және ауа райы жағдайларына байланысты қолдану бойынша шектеулер;

– офлайн әрекеттердің төмен интеллектуалдылығы;

– радио басқару және деректерді беру арналарының төмен жасырындығы;

– құрылымның өміршеңдігі төмен;

– радио басқару арнасы мен ҰҰА спутниктік навигация арнасының радиоэлектрондық кедергілердің әсеріне ұшырауы;

– пайдалы жүктеменің салмағы мен құрамы бойынша шектеулер.

ҰҰА біріктірілген киберфизикалық жүйе негізінде жұмыс істейді, онда датчиктер, жетектер және жердегі басқару пункті арасында деректер алмасу сымсыз байланыс арналары арқылы жүзеге асырылады. Бұл архитектура көптеген осалдықтарды тудырады, бұл шабуылдаушыларға дроннның бағдарламалық және аппараттық компоненттеріне, сондай-ақ олардың арасындағы интерфейстерге, байланыс арналарына шабуыл жасауға және бір уақытта бірнеше элементтерге жан-жақты шабуылдар жасауға мүмкіндік береді – сондықтан бүкіл жүйенің қауіпсіздігін, қорғалуын және ақауларға төзімділігін қамтамасыз ету үшін қорғалған желілік инфрақұрылымды орналастыру және арнайы механизмдерді әзірлеу және енгізу қажет осы саланың бірегей талаптарына сәйкес келетін деректердің киберқауіпсіздігі мен құпиялылығын қамтамасыз ету.

Әрі қарай, киберқауіптердің түрлерін және ҰҰА киберқауіпсіздігін қамтамасыз ету шараларын қарастырыңыз.

Ұшқышсыз ұшу технологиясының қарқынды дамуы олардың қауіпсіздігі мен тұтастығын қамтамасыз етуді маңызды етеді. Жүйенің деректері бірқатар осалдықтарға ие, соның ішінде кибершабуыл қаупі, мысалы, рұқсатсыз кіру, басқаруды ұстап қалу немесе деректерді манипуляциялау.

Бұл қауіпсіздіктің бұзылуына және рұқсатсыз ақпарат жинауға әкелуі мүмкін. Қосымша қиындықтар шектеулі есептеу қуатын, сымсыз байланыс арналарын пайдалануды, құрылғылардың физикалық осалдығын, сондай-ақ қатерлер мен технологиялардың үздіксіз дамуы аясында нормативтік талаптарға және адами факторға сәйкес келу қажеттілігін тудырады.

Кибершабуылдардың нысаны ҰҰА жеке компоненттері де, бүкіл жүйе де болуы мүмкін. Мұндай компоненттерге бағдарламалық жасақтама (БЖ) және аппараттық құралдар жатады: ұшуды басқару жүйелері, байланыс хаттамалары, датчиктер және операциялық жүйелер. Қауіпсіздік пен құпиялылық мәселелері көбінесе шағын ҰҰА жобалау кезеңінде назардан тыс қалады. Көптеген дрондар ашық, шифрланбаған және аутентификацияланбаған деректер арналарын пайдаланатын кіріктірілген сымсыз байланыс модульдерімен жабдықталған, бұл кибершабуылдардың кең ауқымына айтарлықтай осалдықтар тудырады. Дронды бұзғысы келетін зиянкестер әртүрлі әдістерді қолдана алады: көптеген арналарды брондау сұрауларын жіберу, басқару хабарларын ұстау немесе жіберілген деректерді бұрмалау.

Сондай-ақ, көптеген ҰҰА стандартты чиптерден, ашық бағдарламалық жасақтамадан, әмбебап хаттамалардан және архитектуралардан жасалған, мұнда қауіпсіздікке емес, ыңғайлылық пен қол жетімділікке басымдық беріледі. Бұл дрондарды шабуылдаушылар үшін оңай нысанаға

айналдыратын айқын осалдықтарға әкеледі. Мұндай жағдай салаға елеулі қауіп төндіреді, оның дамуына нұқсан келтіреді.

Шабуылдардың салдары шамалы зақымданудан жүйелердің толық істен шығуына дейін, ал ауыр жағдайларда адамдардың өмірі мен мүлкіне қауіп төндіруі мүмкін. Сондықтан киберқауіптерді уақтылы анықтау және бейтараптандыру өте маңызды. Қауіпсіздікті қамтамасыз ету кешенді болуы керек және аппараттың өзін ғана емес, сонымен бірге онымен байланысты барлық инфрақұрылымды қамтуы керек.

Нәтижелер мен талқылаулар.

Жүргізілген талдау ҰҰА үшін ең көп таралған маңызды киберқауіптерді анықтауға мүмкіндік береді. Оларға мыналар жатады: басқаруды ұстап алу (ұрлау), жұмысты тұрақсыздандыру (сәтсіздік) және мәжбүрлі қонуды жүзеге асыру киберқауіпсіздік шабуылдарының ең көп таралған нысандары болып табылады. Бұл қауіптер өте маңызды, өйткені олар дронның өзегіне – оның ұшу және тапсырмаларды орындау қабілетіне соққы береді, бұл тікелей аппараттың өзі мен құнды жүктің жоғалуынан материалдық шығынға, бейнені немесе телеметрияны ұстап қалу арқылы құпия деректердің ағып кетуіне, адамдардың немесе заттардың құлауынан болатын физикалық зақымға, тіпті дронды қару-жарақ ретінде пайдалануға әкеледі.

ҰҰА қауіпсіздігі Wi-Fi, GPS, Bluetooth және ZigBee сияқты осал ашық байланыс технологияларын пайдаланудан туындаған күрделі қауіптерге тап болады. Шабуылдаушылар әртүрлі шабуыл әдістерін қолданады, соның ішінде GPS/Wi-Fi-ны өшіру және бұрмалау, трояндық бағдарламаларды енгізу, таратылған қызмет көрсетуден бас тарту (DDoS) шабуылдары, құпия сөздерді ұрлау, ортадағы адам шабуылдары және жүйелерге рұқсатсыз кіру. Бұл қауіптер басқаруды ұстап қалуға, құпия деректердің ағып кетуіне, жұмысының бұзылуына және тіпті құрылғылардың физикалық жойылуына әкеледі.

Қызмет көрсетуден бас тарту (DoS) және таратылған қызмет көрсетуден бас тарту (DDoS) шабуылдары ұшқышсыз ұшу аппараттарына ең көп таралған қауіп төндіреді, бұл шабуылдардың осы түрлеріне қарсы тиімді механизмдердің болмауына байланысты. DoS шабуылдары жүйенің қол жетімділігінің маңызды бұзылуына әкеледі, мұнда шабуылдаушы мақсатты түрде көптеген сұраныстарды тудырады, бұл дронның желілік инфрақұрылымының шамадан тыс жүктелуіне әкеледі. Мұндай шабуылдар батареяның сарқылуы, процессорға шамадан тыс жүктеме жасау және байланыс арналарының толып кетуі арқылы жүзеге асырылады, бұл жиынтықта айтарлықтай ақаулар тудырады. DDoS шабуылдары жағдайында ҰҰА жүйелері толық қол жетімсіздікке тап болады, өйткені шабуылдаушы көптеген таратылған көздерден жаппай жүктемені ұйымдастырады.

Жеке қауіп – ол навигациялық арналар арқылы жалған деректерді ауыстыру немесе беру арқылы жүзеге асырылатын GPS сигналдарын қолдан жасау. Басқаруды сәтті ұстап алған кезде, шабуылдаушы құрылғыны толық

бақылауға ала отырып, ерікті командаларды енгізе алады. Ұшқышсыз байланыс арналары сеанстарды ұстап қалуға да осал.

Көрсетілген қауіп-қатерлерге қарсы тұру үшін мыналарды қоса алғанда, шаралар кешенін қолдану ұсынылады: сигналдардың түсу бағытын тексеру, берілетін деректердегі бұрмалануларды анықтау және аутентификацияның қатаң хаттамаларын енгізу. Сондай-ақ, киберқауіптердің алдын алуға, анықтауға және оларға жауап беруге бағытталған шаралар кешенін аяқтай отырып, қалыптан тыс белсенділікті бақылауға және анықтауға қызмет ететін интрузияны анықтау жүйесін енгізу. Осылайша, қазіргі заманғы ҰҰА қорғанысы криптографиялық әдістерді, адаптивті қауіпсіздік протоколдарын және нақты уақыт режимінде жұмыс істей алатын интеллектуалды бақылау жүйелерін біріктіруді талап етеді.

3 сурет – Жердегі басқару жүйесіне шабуыл

Сондай-ақ, жердегі басқару жүйесіне жасалған шабуылдар ерекше қауіп төндіреді, өйткені олар шабуылдаушыға арнайы зиянды бағдарламалық жасақтамасы бар компьютер арқылы ұшқышсыз ұшу аппараттарының деректеріне толық қол жеткізуге мүмкіндік береді. Жердегі басқару станциясының компасы зиянды және әдейі бұрмаланған командаларды жіберуге мүмкіндік береді, ал мұндай шабуылдардың типтік орындалуы пернетақтаны, компьютерлік вирустарды және күрделі зиянды бағдарламалық жасақтама кешендерін тіркейтін тыңшы бағдарламалар арқылы жүзеге асырылады. Зиянды басқару командаларын орындау арқылы шабуылдаушы мақсатты ұшқышсыз ұшуды толық басқара алады. Бұл шабуылдар әртүрлі векторлар, соның ішінде әлеуметтік инженерия,

техникалық осалдықтар және зиянды бағдарламалық қамтамасыз ету арқылы дрон деректерінің құпиялылығын бұзады. Рұқсат етілмеген үрдістерге, ұйымдарға және пайдаланушыларға ақпараттың ағып кетуіне жол бермеу үшін кешенді қарсы шараларды қолдану қажет. 3- суретте жердегі басқару жүйесіне шабуыл көрсетілген.

Бұл қауіпті азайтудың тиімді шешімі жердегі басқару жүйелеріне қол жеткізу үшін көп факторлы аутентификацияны енгізу болып табылады, бұл ұшқышсыз ұшуды басқарудың маңызды инфрақұрылымына рұқсатсыз кіруді едәуір қиындатады.

Бұдан басқа, тыңшылық үшін шифрланбаған деректерді ұстау, дұрыс уақытта іске қосылуы мүмкін зиянды бағдарламаны енгізу және өндіріс кезеңінде дрондардың барлық партияларын осалдықтармен жұқтыратын жеткізу тізбегіне шабуылдар сияқты басқа да маңызды қауіптер бар.

Бұл қауіптермен күресу әр түрлі шараларды қажет етпейді, бірақ барлық байланыс арналарын міндетті түрде шифрлауды, құрылғылардың қатаң аутентификациясын, резервтік навигациялық жүйелермен GPS спуфингінен қорғауды, ұшу аймақтарын шектеу үшін географиялық аймақтарды пайдалануды, қауіпсіз апаттық қайтаруды қамтамасыз етуді және осалдықтарды жою үшін бағдарламалық жасақтаманы үнемі жаңартуды қамтитын кешенді тәсіл. Осылайша, ҰҰА қорғау – бұл құрылғының өмірлік циклінің барлық кезеңдерінде, дизайннан бастап күнделікті жұмысына дейін киберқауіпсіздікті ескеруі керек үздіксіз үрдіс.

Қорытынды.

Қазіргі заманғы ұшқышсыз ұшу аппараттарының қауіпсіздік жүйелері киберқауіптердің қарқынды дамуына және платформалардың технологиялық шектеулеріне байланысты көп қырлы қиындықтарға тап болады. Негізгі тәуекелдерге байланыс арналарының осалдығы, деректерді криптографиялық қорғаудың болмауы, жердегі басқару станцияларына рұқсатсыз кіру мүмкіндігі және кескін басқыншыларын пайдалану салдарынан құпиялылықты бұзу қаупі жатады. GPS-спуфинг, байланыс сеанстарын тоқтату және ҰҰА жұмыс істеу қабілетті таратылған қызмет көрсетуден бас тарту (DDoS) шабуылдары ерекше қауіп төндіреді. Бұл мәселелерді шешу технологиялық, нормативтік және ұйымдастырушылық шараларды біріктіретін кешенді тәсілді қажет етеді. Қорғаудың негізгі элементтері: жеңіл криптографиялық алгоритмдерді енгізу (эллиптикалық қисықтар мен бір раундтық функцияларға негізделген), адаптивті аутентификация хаттамаларын қолдану, жасанды интеллект компоненттерімен анықтау жүйелерін енгізу, ұшу жолдарын оңтайландыру. Бұл мақалада ұшқышсыз ұшу жүйелеріндегі киберқауіпсіздікке шолу талқыланды.

Осылайша, ұшқышсыз ұшу жүйелеріндегі киберқауіпсіздік зерттеушілердің назарын қажет ететін сала болып қала береді. Соңғы жылдары кибершабуылдар саны экспоненциалды түрде өсуде. Сондықтан ҰҰА құрастырушылар, компьютерлік қауіпсіздікті пайдаланушылар мен

зерттеушілер тиісті қауіпсіздік шараларын қабылдау үшін киберқауіпсіздік саласындағы соңғы оқиғалардан хабардар болуы керек. ҰҰА киберқауіпсіздігін арттыру сұрақтарын келесі басылымдарда толығырақ зерттеп, сипаттайтын боламыз.

Қаржыландыру: зерттеу ГҚ № AP26101065 жобасы шеңберінде жүргізілді.

ӘДЕБИЕТТЕР

1. Noor, F.; Khan, M.A.; Al-Zahrani, A.; Ullah, I.; Al-Dhlan, K.A. A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics. Drones 2020, 4, 65.

2. Ahmed, F.; Mohanta, J.C.; Keshari, A.; Yadav, P.S. Recent Advances in Unmanned Aerial Vehicles: A Review. Arab. J. Sci. Eng. 2022, 47, 7963–7984.

3. Majeed, S., Sohail, A., Qureshi, K. N., Iqbal, S., Javed, I. T., Crespi, N., et al. (2022). Coverage area decision model by using unmanned aerial vehicles base stations for ad hoc networks. Sensors 22, 6130. Doi: 10.3390/s22166130

4. Khan, A., Gupta, S., and Gupta, S. K. (2022). Emerging UAV technology for disaster detection, mitigation, response, and preparedness. J. Field Robotics 39, 905–955. doi:10.1002/rob.22075

Gulzhan Kashaganova, PhD, associate professor, Satpayev University, Almaty, Kazakhstan, guljan_k70@mail.ru

Dina Satybaldina, candidate of physical and mathematical sciences, professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, dinasaty@gmail.com

Maral Zhasandikyzy, PhD, International University of Transport and Humanities, Almaty, Kazakhstan

UAV CYBERSECURITY THREATS RESEARCH

Abstract. Over the past ten years, the study of UAVs (UAVs) has expanded significantly due to their unique properties and numerous use cases in the military, agriculture, monitoring, monitoring, video photography and other industries. Despite its widespread use, UAVs face serious cybersecurity challenges. UAS are vulnerable to various cyber attacks because they are complex systems in which the cybernetic and physical components are closely related. Attackers can attack these components, interfaces between them, wireless communication channels, or a combination of the two. The main cyber threats of the UAV are unauthorized access and seizure of control, theft or leakage of collected data, as well as data falsification (deception), allowing attackers to control the device. The questions of developing reliable protection measures, such as encryption systems for data

protection, authentication mechanisms for authentication, cyber threats analysis and prediction algorithms for detecting anomalies, are discussed in this article.

Keywords: UAV, cybersecurity, cyber attacks, protection measures.

Гулжан Кашаганова, PhD, ассоциированный профессор, Satbayev University, Алматы, Казахстан, guljan_k70@mail.ru
Дина Сатыбалдина, к.ф.-м.н., профессор, L.N. Gumilyov Eurasian National University, Астана, Қазақстан, dinasaty@gmail.com
Марал Жасандықызы, PhD, International University of Transport and Humanities, Алматы, Казахстан

ИССЛЕДОВАНИЕ УГРОЗ КИБЕРБЕЗОПАСНОСТИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Аннотация. За последние десять лет исследования беспилотных летательных аппаратов (БПЛА) значительно расширились из-за их уникальных свойств и множества вариантов использования в военной области, сельском хозяйстве, мониторинге, контроле, видео-фотосъемке и других областях. Несмотря на широкое использование, БПЛА сталкивается с серьезными проблемами кибербезопасности. БПЛА уязвимы для различных кибератак, поскольку они представляют собой сложные системы, в которых кибернетические и физические компоненты тесно связаны. Злоумышленники могут атаковать эти компоненты, интерфейсы между ними, каналы беспроводной связи или их комбинацию. Основными киберугрозами БПЛА являются несанкционированный доступ и получение контроля, которые позволяют злоумышленникам управлять устройством, кража или утечка собранных данных, а также фальсификация (обман) данных. В этой статье рассматриваются вопросы разработки надежных защитных мер, таких как системы шифрования для защиты данных, механизмы аутентификации для аутентификации, а также алгоритмы анализа и прогнозирования киберугроз для выявления аномалий.

Ключевые слова: беспилотный летательный аппарат, кибербезопасность, кибератаки, меры защиты.

Қабылданған күні: 2025 жылғы 05 қазан
Рецензиядан өткен күні: 2026 жылғы 03 ақпан
Мақұлданған күні: 2026 жылғы 01 наурыз