Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-7263. eISSN: 2663-1261
ТЕХНИКАЛЫҚ ҒЫЛЫМДАР ЖӘНЕ ТЕХНОЛОГИЯЛАР СЕРИЯСЫ /
TECHNICAL SCIENCES AND TECHNOLOGY SERIES/
СЕРИЯ ТЕХНИЧЕСКИЕ НАУКИ И ТЕХНОЛОГИИ

МРНТИ 73.37.81 https://doi.org/10.32523/2616-7263-2024-149-4-104-118
Ғылыми мақала

Ұшқышсыз ұшу аппараттары арқылы өрт ошақтарын бақылау және алынған сигналдарды коммуникациялауда ақпараттық қорғау

А.М.Молдамурат[1], Д.М.Калманова[2], А.Байманова*[2], Х.Молдамурат[2], Г.А.Бегимова[2]

[1]ТОО «Қазмедиа орталығы» Басқару компаниясы», Астана, Қазақстан
[2] Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

*(E-mail: *dinara_kalmanova@mail.ru)*

Аңдатпа. Бұл мақалада ұшқышсыз ұшу аппараттарын (ҰҰА) сенсорлық датчиктермен жабдықтау арқылы өрт ошақтарын бақылау және коммуникация жүйесін ақпараттық қорғау туралы жазылған. ҰҰА сенсорлық датчиктермен жабдықталғандықтан, өртті бақылауда датчиктерден алынған сигналдарды орталыққа жіберу және оның коммуникация жүйесінің ақпараттық қорғалуы қарастырылады. Дала өрттері мен басқа да өрт түрлерін экологиялық апаттарға байланысты қауіптердің артуымен тиімді бақылау және басқару әдістері көрсетілген. Бұл, ҰҰА-ны өрт ошақтарын бақылауда таптырмас құралға айналдырады. Дегенмен, бұл технологияларды пайдалану деректердің жоғалу тәуекелімен және байланыстың бұзылуымен бірге келеді. Мақалада шифрлау, аутентификация және кибершабуылдан қорғауды қоса алғанда, ақпаратты беру қауіпсіздігі мен сенсорлық деректерді басқару жүйесімен біріктірудің заманауи тәсілдері талданады. Байланыс жүйесін кешенді қорғауды құру бойынша ұсыныстар беріледі, бұл дағдарыс жағдайында басқарудың сенімділігі мен тиімділігін арттыруға мүмкіндік береді. ҰҰА жүйесінің жұмыс істеуінің негізгі принциптері, соның ішінде шешім қабылдау алгоритмдері және бір желідегі бірнеше ұшқышсыз ұшу аппараттарының әрекеттерін үйлестіру сипатталған. Маршруттарды оңтайландыру, тапсырмаларды орындау тиімділігін арттыру әдістері қарастырылған. Сонымен қатар, ұшқышсыз ұшу аппараттарын сенсорлық датчиктермен жабдықтау арқылы орман өрттерін бақылау тиімділігі айтылады. ҰҰА интегралды бағдарламалық кешенінің интеллектуалды басқару жүйесі берілген. ҰҰА аудиосигнал арқылы басқаруда ChaCha20 деректерді беру қауіпсіздігін қамтамасыз етудің сенімді механизмінің алгоритм шифрлеу әдістері ұсынылған.

Түйін сөздер: ұшқышсыз ұшу аппараттары (ҰҰА), сенсорлық датчиктер, өртті бақылау, ақпараттық қауіпсіздік, коммуникация жүйесі, шифрлау алгоритмдері, киберқауіпсіздік.

Түсті 28.09.2024. Жөнделді 18.10.2024. Мақұлданды 13.11.2024. Онлайн қолжетімді 31.12.2024

[1]*Хат хабар үшін авторы

Кіріспе

Бұл жұмыста топтық басқарумен ұшқышсыз ұшу аппараттарын сенсорлық датчиктермен жабдықтау арқылы орман өрттерін бақылау және ұшқышсыз ұшу аппараттарының (ҰҰА) интеграцияланған бағдарламалық кешенін интеллектуалды басқару қарастырылады.

Орман өрттері экожүйелерге, экономикаға және адамдардың қауіпсіздігіне үлкен қауіп төндіреді. Өртті бақылау мен басқарудың дәстүрлі әдістері көбінесе тиімсіз. Осыған байланысты сенсорлық датчиктері бар ұшқышсыз ұшу аппараттарын пайдалану бұл мәселені шешудің өзекті әдісіне айналуда [1].

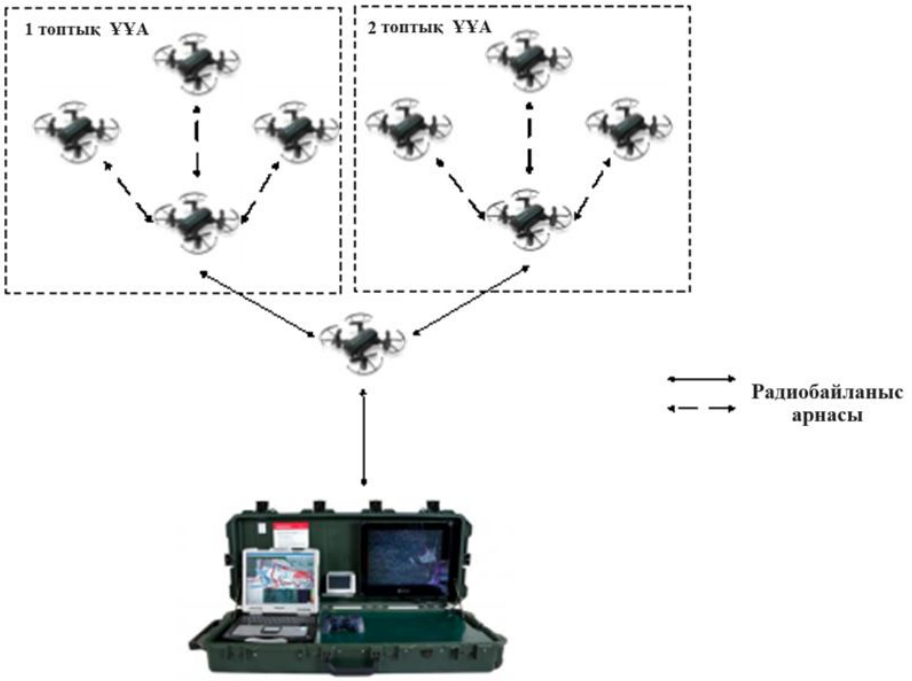
Мониторингте ҰҰА қолдану әртүрлі сенсорлық датчиктермен (жылу камералары, оптикалық датчиктер, ауа сапасының датчиктері) жабдықталған аппараттардың өрттің алғашқы белгілерін тез және тиімді анықтауына мүмкіндік береді. Олар жедел әрекет етуді қамтамасыз етіп, өрт ошақтарын анықтау уақытын азайта отырып, кең аумақтарды патрульдей алады.

Технологияның артықшылықтарына келетін болсақ, тиімділік, қауіпсіздік және дәлдік маңызды рөл атқарады:

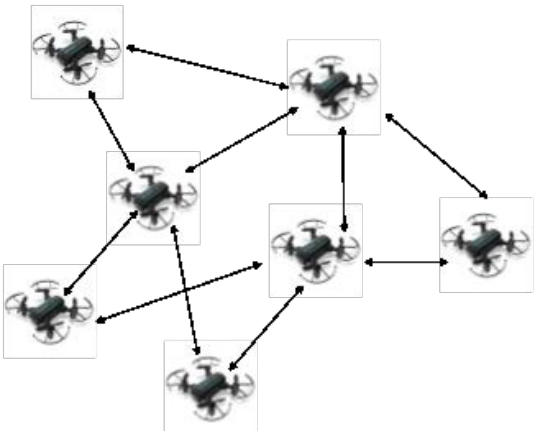
о Тиімділік: ұшқышсыз ұшу аппараттары қысқа уақыт ішінде үлкен аумақтарды қамтып, өрттің ауқымын жылдам анықтауға және бағалауға мүмкіндік береді.

о Қауіпсіздік: ұшқышсыз ұшу аппараттарын пайдалану адамдар үшін қауіпті азайтады, себебі олар қауіпті жерлерде бақылау жүргізе алады.

о Дәлдік: ауадан алынған сенсорлық деректер температураны және өрттің таралуын жоғары дәлдікпен және егжей-тегжейлі анықтауға мүмкіндік береді [2].



1-сурет. ҰҰА басқару және жербеті станциямен байланыс



2-сурет. Орталықтандырылмаған (шеткі) басқарудағы ҰҰА өзара әрекеттесу схемасы

ҰҰА күрделі тапсырмаларды аз уақыт пен ресурстарды жұмсай отырып орындау қабілетінің арқасында көптеген салалардың ажырамас бөлігіне айналуда. ҰҰА-ны әртүрлі сенсорлармен жабдықтау қоршаған ортаны бақылау, ауыл шаруашылығы, қауіпсіздік және басқа да көптеген салаларда жаңа көкжиектерді ашады.

Әдіснама

ҰҰА сенсорлық датчиктерін пайдалану [3, 14]

1. Қоршаған ортаны бақылау құрылғысы бейне бақылау датчигі – сенсорлық датчиктермен жабдықталған ҰҰА ауаның ластану деңгейі немесе су сапасы сияқты экожүйелердегі өзгерістерді қашықтан бақылай алады.

2. Ауыл шаруашылығында қолданылатын сенсорлық датчиктер – датчиктер дақылдардың ылғалдылық жағдайын бағалауға, алқаптың температурасын диагностикалауға мүмкіндік береді, бұл ауыл шаруашылығында өнімділіктің қауіпсіздігін уақытылы бағалауға және өнімнің жоғарылауына ықпал етеді.

3. Қауіпсіздік жүйелерінде қолданылатын сенсорлық датчиктер – камера, тепловизор, газ анализаторы, ауа ылғалдылығы және температура датчиктері бар ҰҰА орман өрттерін бақылау және алдын алу, іздеу-құтқару операциялары және шекараны қорғау үшін қолданылады.

4. Геодезия және картография – сенсорлар қала құрылысы мен жер ресурстарын басқаруға қатысты жоғары дәлдіктегі карталар мен рельефтің үш өлшемді модельдерін жасауға көмектеседі.

1-кесте. Орман өртін анықтауға арналған NB-IoT терминалында қолданылатын сенсорлық датчиктердің түрлері

Температура мен ылғалдылық сезетін әмбебап датчигі

Тепловизор жоғарғы температураның жылуын сезіну датчигі

Газанализатор датчигі

Түтінді сезінетін датчигі

Қашықтықтан сезетін көлденең сәулелік Фотоэлектрлі сенсорлы датчигі

ҰҰА сенсорлық датчиктерінің артықшылықтарына қол жетімділік, уақыт пен ресурстарды үнемдеу, деректердің дәлдігі мен егжей-тегжейі, сондай-ақ қауіпсіздік жатады. ҰҰА дәстүрлі бақылау әдістері тиімсіз болатын жету қиын және қауіпті жерлерге жете алады. Деректерді жедел алу шешім қабылдау процестерін едәуір жылдамдатады. Сенсорлық датчиктер терең талдауға мүмкіндік беретін жоғары деңгейдегі егжей-тегжейлі ақпаратты қамтамасыз етеді. Сонымен қатар, ұшқышсыз ұшу аппараттарын пайдалану, әсіресе қауіпті аймақтарда, адамдар үшін қауіп-қатерді азайтады [4, 11].

3-сурет. ҰҰА басқару жүйесінің негізгі жұмыс жасау принципі

Бұл жұмыста ұшқышсыз ұшу аппаратының (ҰҰА) интегралды бағдарламалық кешенінің интеллектуалды басқару жүйесін қорғау және модельдеу қарастырылады. Технологиялардың дамуымен, әсіресе әскери және азаматтық салаларда ҰҰА-ның қолданылуымен, деректерді басқару мен қорғаудың сенімді жүйесін құру маңызды.

Жұмыс бірнеше ҰҰА-ны үйлестіру мен өзара әрекеттесуін қамтамасыз ететін интеллектуалды басқару архитектурасын әзірлеуге бағытталған. Бағдарларды оңтайландыру және тапсырмалардың тиімділігін арттыру үшін жасанды интеллект алгоритмдерін қолдану басты назарда. Деректерді қорғау үшін шифрлау мен аутентификацияны қамтитын кешенді әдістер пайдаланылады, бұл ақпараттың қауіпсіздігін қамтамасыз етеді.

Жүйені модельдеу ҰҰА-ның өзара әрекеттесуі сценарийлерін зерттеуге мүмкіндік береді, осылайша осалдықтар мен қауіптер анықталады. Ұсынылған модельдің жоғары тиімділігі мен автоматтандыру жүйелерін басқарудағы функционалдылықты кеңейту әлеуеті көрсетіледі.

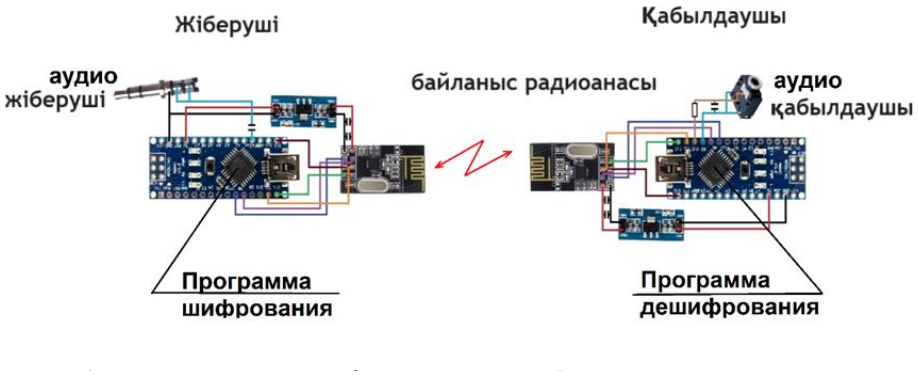
ҰҰА интегралды бағдарламалық кешенінің қорғау стандарттары арнайы енгізіледі, бұл ҰҰА-ның жер беті басқару орталығымен байланысындағы қауіпсіздікті қамтамасыз етеді. Басқарудың барлық түрлері, соның ішінде интеллектуалды басқару микроконтроллер арқылы жүзеге асырылады, ол ҰҰА-ның кешендік басқару орталығы болып табылады [5].

ҰҰА арнайы дыбыстық басқаруда арнайы ArduinoEncryptor бағдарламасында әзірленген пакеті (.cpp) – бұл ГОСТ 28147-89 алгоритмінің модификациясы негізінде жасалған ақпараттық қорғау үшін шифрлау пакеті (аутентификациямен). Модификация Arduino микроконтроллерінің шектеулі есептеу ресурстарын ескере отырып, төмен бит, төмен өнімділік, регистр жадын пайдалану және т.б. пакеттің құрамына модульдің интерфейсіне кіретін мүмкіндіктер кіреді:

–шифрды іске асыру (криптопримитив);

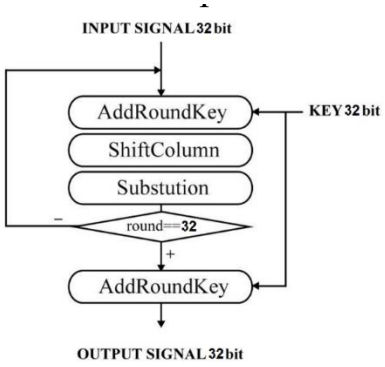
–есептегіш режимінде шифрлауды жүзеге асыру (гаммалау);

–CMAC (NIST SP 800-38B) алгоритмінің деректерін аутентификациялау схемасын енгізу.



4-сурет. Аудиодеректерді криптографиялық қорғауды жүзеге асырудың мысалы: Arduino микроконтроллер платформасына негізделген

Ал енді радиобайланыс арқылы байланысқа түсудегі ақпараттық қорғау арнайы радиостанцияларға арналған IP екі саннан тұрады (мысалы, IP54). Бірінші сан қатты денелерден, екіншісі сұйықтықтан қорғауды білдіреді. Шаң мен ұсақ бөлшектерден қорғаудың 6 дәрежесі және ылғалдан қорғаудың 8 дәрежесі бар. ГОСТ Р 50829-95 радиостанциялардың, радиоэлектрондық аппаратураның трансивер аппаратурасы және олардың құрамдас бөліктерін пайдалана отырып, қауіпсіздігі осы халықаралық стандартпен бекітілген [6, 10].



5-сурет. Деректерді шифрлау алгоритмінің схемасы

Аутентификация үшін CMAC (NIST SP 800-38B) алгоритмі қолданылады. Хабарламаның құрамына аутентификация кодын (имитациялық кірістіру) есептеу үшін NONCE мәні қосылады. Дәл сол NONCE мәні негізгі ағынды құру үшін қолданылуы керек. Берілген шифрлау кілтімен NONCE тек бір рет пайдаланылуы мүмкін. Қауіпсіз деректерді бөлісетін түйіндер синхронды NONCE мәнін пайдаланады деп болжануда. Бұл мән хабарламамен бірге ашық түрде берілуі мүмкін.

Жалпы қолданыстағы шифрлеу алгоритмдері:

– Симметриялық: AES, ГОСТ Р 34.11-94, DES, Twofish, IDEA және т.б.

– Жеңіл шифрлау: ChaCha20, Salsa20 және т.б.

– Асимметриялық: RSA, ElGamal және т.б.

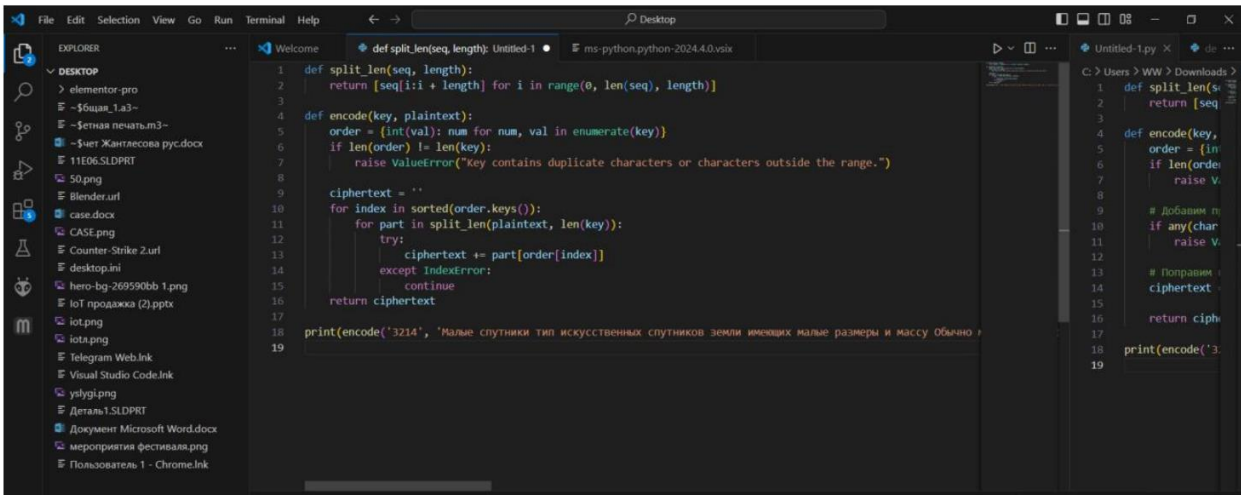
– Хэш-функциялар: MD4, MD5 және т.б.

– Транспозициялық шифрлеу алгоритмдері және т.б.

Транспозициялық шифр әдісі – шифрланған мәтінді қалыптастыру үшін ашық мәтіндегі алфавиттердің реті қайта реттелетін криптографиялық алгоритм. Бұл процеске қарапайым мәтіннің нақты алфавиттері енгізілмейді [7].

Нәтижелер мен талқылау

Бағдарламалық Visual Studio ортасында Python 3.12.3 бағдарламалық тілінде кодтың негізгі ҰҰА басқарудағы локациялық жүйесінің нұсқасы жасалады және ақпарат ағымының алгоритмі жасалады. ҰҰА басқару жүйесінде инициализация орындалады, координаттар жаңартылады және көрсетіледі, содан кейін жүйе өшіріледі. Деректерді қорғау жүйесін (ДПЖ) біріктіруге арналған код берілген. Бұл үшін ҰҰА тобын әзірлейміз, өзара ақпарат алмасуда деректерді шифрлау және шифрын ашу әдістерін қамтитын жүйелер құрамыз және сондай-ақ, жүйенің күйін тексеру үшін тестілеу жүйесін іске асырамыз. Барлық жүйелерді біріктіру үшін (интеллектуалды басқару, орналасу және қорғау) бірыңғай бағдарламалық жасақтама кешенінде біз топтасқан ҰҰА сыныбын құрамыз. Осы жүйелердің әрқайсысымен өзара әрекеттесу процесін іске асырамыз. Бұл бізге ҰҰА-ны орталықтан басқаруға мүмкіндік береді және интеграциясын орындауға болады [8, 9].



6-сурет. Python бағдарламалық тілде кодтарды жазу тақтасы

ҰҰА топтық сыныбын қолданудағы мысалы: Кодтың негізгі бөлігінде бірыңғай бағдарламалық кешеннің данасы жасалады, инициализация жүзеге асырылады, кешеннің жұмысы басталады және соңында барлық жүйелер сөндіріледі.

Листинг: бағдарлама үзіндісі.

Интеллектуалды басқару бағдарламалық модуль жүйелерін интеграциялау (Siu):

class IntelligentControlSystem:

def _init_(self, name):

Жүйені берілген атпен инициализациялау

self.name = name

self.Модульдер = [] # Топттық ҰҰА жүйе модульдерін сақтауға арналған тізім

self.active_modules = [] # белсенді модульдерді сақтауға арналған тізім

def add_module(self, module):

Жүйеге модуль қосу әдісі

self.modules.append(module)

Print (F " Модуль {module.name} Топттық ҰҰА жүйеге қосылды {self.name}.")

def remove_module(self, module):

Модульді жүйеден жою әдісі

if module in self.modules:

self.modules.remove(module)

Print (F " Модуль {module.name} Топттық ҰҰА жүйеден жойылды {self.name}.")

else:

Print (F " Модуль {module.name} Топттық ҰҰА жүйеде табылған жоқ. ")

def integrate(self):

Барлық модульдерді жүйеге біріктіру әдісі

for module in self.modules:

try:

print (F " модульді біріктіру {module.name}...")

```
module.initialize () # Топтық ҰҰА басқару модульді инициализациялау
self.active_modules.append (module) # тізімге белсенді модуль қосу
except Exception as e:
# Егер Топттық ҰҰА басқару модульді инициализациялау сәтсіз болса, қателерді өңдеу
print (F " Топттық ҰҰА басқару модульді біріктіру кезіндегі қате {module.name}: {e}")
```

ҰҰА басқару жүйелерінде дыбыстық сигналдарды қорғау үшін ChaCha20 шифрлау алгоритмі қолданылады. Аудио сигналдар оператор мен ҰҰА арасындағы маңызды өзара әрекеттестікті қамтамасыз етеді, бірақ ашық түрде беру рұқсатсыз қол жеткізу қаупін тудырады. ChaCha20 алгоритмі жоғары жылдамдығы және шабуылдарға төзімділігімен таңдалды [9].

Әзірлеу аясында синусоидалы аудио сигналдарды генерациялау, оларды ChaCha20 арқылы шифрлау және шифрын ашу әдістері зерттелді. Алгоритмнің практикалық қолдануы деректерді қорғауда сенімді шифрлау мүмкіндігін көрсетті. Эксперимент нәтижелері ChaCha20 тиімділігін растады: шифрланған аудио сигналдар сапасын жоғалтпай сәтті жіберілді және декодталды, бұл алгоритмнің практикалық қолданылуын дәлелдейді [12].

ҰҰА аудиосигнал арқылы басқаруда ChaCha20 деректерді беру қауіпсіздігін қамтамасыз етудің сенімді механизмінің алгоритм шифрлеуі төменде көрсетілген.

```
from Crypto.Cipher import ChaCha20
from Crypto.Random import get_random_bytes
аудио файлдармен жұмыс істеу үшін soundfile as SF # импорттаңыз
import os
# Дыбыстық сигнал параметрлері
fs = 44100 # іріктеу жылдамдығы
ұзақтығы = 5 # ұзақтығы секундпен
frequency = 440 # сигнал жиілігі (Ла) Гц
# Синусоидалы сигнал генерациясы
t = np.linspace(0, duration, fs * duration, endpoint=False)
audio_signal = 0.5 * np.sin(2 * np.pi * frequency * t)
# 16 биттік бүтін санға түрлендіру (signed) және дискіге сақтау
audio_signal_int16 = np.int16(audio_signal * 32767)
sf.write('original_audio.wav', audio_signal_int16, fs)
# Шифрлауға дайындық
key = get_random_bytes (32) # 256 биттік кілт
nonce = get_random_bytes (8) # 64 биттік IV
# Аудио сигналды шифрлау
cipher = ChaCha20.new(key=key, nonce=nonce)
ciphertext = cipher.encrypt(audio_signal_int16.tobytes())
# Шифрланған аудио сигналды дискіге сақтау
with open('encrypted_audio.bin', 'wb') as f:
f.write(nonce + ciphertext)
```

Код 440 Гц жиіліктегі 5 секундтық синусоидалы дыбыстық сигналды жасайды, бұл

сигнал WAV форматында сақталады. Синусоидалы сигнал – дыбыстық толқынның негізгі түрі, оны генерациялау үшін numpy кітапханасы пайдаланылады. Шифрлау процесінде ChaCha20 алгоритмі шифрлау нысаны ретінде қолданылады. Алгоритмге бірегей кілт және бастапқы вектор (IV) беріледі. Аудио сигнал байттарға түрлендіріледі және шифрланады. Шифрланған аудио сигналды сақтау кезінде IV, тег және шифрланған деректер файлға жазылады, бұл деректерді кейін декодтау үшін қажет. Декодтау барысында шифрланған деректер файлдан оқылып, бұрын берілген кілт пен IV арқылы декодталады. Декодталған аудио сигнал жаңа WAV файлына сақталады. WAV форматы аудио файлдарды сақтау үшін кеңінен қолданылып, көптеген медиа ойнатқыштармен ойнатуға мүмкіндік береді [13].

Ескертулер ретінде, бұл код ChaCha20 алгоритмімен аудио сигналды шифрлау мен шифрды шешудің негізгі принциптерін көрсетеді. Нақты жағдайларда қателерді өңдеу, кілттерді басқару және деректердің тұтастығын қамтамасыз ету сияқты қосымша факторларды ескеру қажет. Аудио файлдарды ойнату үшін WAV пішімін қолдайтын кез келген медиа ойнатқышты пайдалануға болады.

Бұл зерттеу ҰҰА басқару жүйелеріндегі аудио сигналдарды шифрлаудың маңыздылығын көрсетеді. ChaCha20 алгоритмі деректерді беру қауіпсіздігін қамтамасыз етудің сенімді механизмі ретінде тиімділігін дәлелдейді. Жұмыс нәтижелері пилотсыз технологиялар контекстінде ақпараттық қауіпсіздікті одан әрі зерттеуге негіз бола алады. ҰҰА басқаруды қорғау үшін ChaCha20 шифрлау алгоритмін пайдалану берілетін аудио сигналды қауіпсіздікпен қамтамасыз етеді. Демонстрация ретінде біз аудио сигналды генерациялау, тасымалдау үшін шифрлау және шифрын ашу процесін көрсете отырып, мысал жасап ұсынамыз [15].

Қорытынды

Ұшқышсыз ұшу аппараттарын сенсорлық датчиктермен жабдықтау орман өрттерін бақылаудың тиімді тәсілі болып табылады. Бұл технология жедел жауап беру мен басқарудың жоғары тиімділігін қамтамасыз етеді. Болашақта ҰҰА деректерін болжау және ескерту жүйелерімен біріктіру орман ресурстарын қорғауды айтарлықтай жақсартады, өрт белсенділігін төмендетеді. Жүйенің негізгі принциптері, шешім қабылдау алгоритмдері және бір желідегі бірнеше ҰҰА әрекеттерін үйлестіру сипатталған. Маршруттарды оңтайландыру мен тапсырмаларды орындау тиімділігін арттыру үшін жасанды интеллект әдістерінің маңызы атап өтіледі. Зерттеу нәтижелері топтық басқаруды сәтті жүзеге асыру мүмкіндігін көрсетіп, ҰҰА-ны бақылау, барлау және логистикада қолданудың жаңа перспективаларын ашады.

Сенсорлық датчиктерді пайдалану арқылы өрт ошақтарын бақылау, алынған деректерді қауіпсіз орталыққа жеткізу қарастырылған. Аудио сигналдарды қорғау үшін ChaCha20 шифрлау алгоритмі сәтті қолданылды. Эксперимент нәтижелері алгоритмнің жоғары жылдамдығы мен беріктігін растады, шифрланған аудио сигналдар сапасын жоғалтпай қауіпсіз түрде жіберілді. Бұл деректерді беру қауіпсіздігін қамтамасыз етудегі шифрлаудың маңыздылығын көрсетеді. Нәтижелер ҰҰА контекстіндегі ақпараттық

қауіпсіздік зерттеулеріне жаңа мүмкіндіктер ашады, ресурстарды тиімді басқару, операцияларды қауіпсіз жүргізу және қоршаған ортаны қорғауға инновациялық шешімдер ұсынады.

Мақалада ҰҰА интегралды бағдарламалық кешенінің басқару алгоритмі ұсынылған. Ақпараттық қорғау микроконтроллерлік жүйеде іске асырылып, алгоритм көрсетілген. Visual Studio ортасында Python бағдарламалық тілінде код жазылып, шифрлау мен дешифрлеу жүзеге асырылды. ҰҰА кешендік жүйесінің интеллектуалды басқару моделі құрылды. Деректерді қорғау жүйесін (SZD) халықаралық стандарт хаттамалары негізінде бағдарламалық кодпен бірге мысалдар келтірілген. Жұмыс нәтижелері ақпараттық деректерді қорғаудың жоғары тиімді механизмдерін күрделі операциялық жағдайларда қолдануға мүмкіндік береді, бұл ҰҰА қауіпсіздігі мен функционалдығын арттыруға ықпал етеді. Осы әдістерді дамыту мобильді объектілердегі интеллектуалды басқару мен ақпараттық қорғау технологияларын әртүрлі салаларда қолдану үшін жаңа мүмкіндіктер ашады.

Алғыс айту, мүдделер қақтығысы

Бұл зерттеу Қазақстан Республикасы Ғылым және Жоғары білім министрлігінің Ғылым Комитеті тарапынан қаржыландырылды (Жоба ИРН № AP23486167). Авторлар осы мақалаға қатысты ешқандай мүдделер қақтығысы жоқ екенін мәлімдейді және зерттеу барысында көрсетілген қолдау мен ынтымақтастық үшін барлық әріптестер мен мекемелерге ризашылығын білдіреді.

Авторлардың қосқан үлесі:

А.М. Молдамурат, Д.М. Калманова, Х. Молдамурат – тұжырымдама, әдістеме, ресурстар, мәліметтер жинау.

А. Байманова, Г.А. Бегимова – талдау, визуализация, интерпретация, жазу, өңдеу.

Әдебиеттер тізімі

1. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. — Pearson, 2017.

2. Diffie W., Martin E. New Directions in Cryptography // IEEE Transactions on Information Theory. – 1976. – Т. 22, № 6. – С. 644-654.

3. Атанов С.К., Сейткулов Е.Н., Молдамурат Х., Ергалиева Б.Б., Балбаев Г.К., Оспанов Р.М. Ұялы байланыс және сымсыз жүйелер дабылдарын интеллектуальды түрде басуға арналған құрылғы, Патент № 8530, 2023/0753.2, 06.07.2023. – РГП «Национальный институт интеллектуальной собственности», Республика Казахстан.

4. Khamis M.A., Kamel W.A. Drone Security: Issues and Challenges // International Journal of Computer Applications. – 2018. – Т. 182, № 30. – С. 1-7.

5. Молдамурат Х., Мақыш С.Б., Атанов С.К., Бақыт М.А. Устройство криптографически защищённого управления мобильным роботом, Патент № 9067, 2024/0437.2, 26.04.2024. – РГП «Национальный институт интеллектуальной собственности».

6. Cheng G., Kwan C. Security Problems in UAV Applications // IEEE Communications Magazine.– 2015. – Т. 53, № 4. – С. 54-59.

7. Moldamurat K., Seitkulov Y., Atanov S., Bakyt M., Yergaliyeva B. Enhancing Cryptographic Protection, Authentication, and Authorization in Cellular Networks: A Comprehensive Research Study // International Journal of Electrical and Computer Engineering. – 2024. – Т. 14, № 1. – С. 479-487.

8. Әлмағанбет Т.Ш., Асқарбек М.А., Атанова А.А. Ғарыш саласында криптоқорғау жүйесін пайдаланудың маңыздылығы мен ерекшеліктері // XIX Международная научная конференция студентов и молодых ученых «Ғылым және білім – 2024». – ISBN 978-601-7697-07-5. – С. 203-211.

9. Zhang X., Wang Y. Multisensor Data Fusion for Fire Detection in Urban Fire Control using UAVs // Sensors. – 2019. – Т. 19, № 4. – С. 936.

10. Pimentel A.R., et al. Aerial Detection of Fires Using Drones and Infrared Cameras: A Case Study // Journal of Fire Sciences. – 2016. – Т. 34, № 2. – С. 145-161.

11. Anderson K., Gaston G. Lightweight Drones: Development of an Unmanned Aerial Vehicle (UAV) for Environmental Monitoring // Remote Sensing. – 2013. – Т. 5, № 7. – С. 3279-3297.

12. Lague D., Bouchard M. UAVs for Monitoring and Assessing the Impact of Forest Fires // Remote Sensing. – 2017. – Т. 9, № 1. – С. 50.

13. Bakyt M., Moldamurat K., Konyrkhanova A., Maidanov A., Satybaldina D. Integration of Cryptography and Navigation Systems in Unmanned Military Mobile Robots: A Review of Current Trends and Perspectives // CEUR Workshop Proceedings. – 2024. – Т. 3680.

14. Sigh V., Raghunathan M. Security and Privacy Issues in Drone Technology: A Survey // IEEE Access. – 2020. – Т. 8. – С. 23249-23272.

15. Zhang Q., et al. Survey on Firewall Technologies in UAV Networks // Future Generation Computer Systems. – 2020. – Т. 105. – С. 375-385.

А.М.Молдамурат[1], Д.М.Калманова[2], А.Байманова*[2], Х.Молдамурат[2], Г.А.Бегимова[2]

[1]ТОО «Управляющая компания «Қазмедиа орталыгы», Астана, Казахстан

[2]Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан

Контроль очагов пожара и информационная защита при коммуникации полученных сигналов с помощью беспилотных летательных аппаратов

Аннотация. В этой статье рассказывается об информационной защите системы мониторинга и коммуникации очагов пожара путем оснащения беспилотных летательных аппаратов (БПЛА) сенсорными датчиками. Поскольку БПЛА оснащена сенсорными датчиками, при контроле пожара предусматривается передача сигналов от датчиков в центр и информационная защита его коммуникационной системы. Показаны эффективные методы контроля и управления лесными пожарами и другими видами пожаров с увеличением рисков, связанных с экологическими бедствиями. Это делает БПЛА незаменимым инструментом в контроле очагов пожаров. Однако использование этих технологий сопряжено с риском потери данных и нарушения связи. В статье анализируются современные подходы к интеграции безопасности передачи информации и сенсорной системы управления данными, включая шифрование, аутентификацию и защиту от

кибератак. Даны рекомендации по созданию комплексной защиты системы связи, что позволит повысить надежность и эффективность управления в условиях кризиса. Описаны основные принципы функционирования системы БПЛА, включая алгоритмы принятия решений и координацию действий нескольких беспилотных летательных аппаратов в одной сети. Рассмотрены методы оптимизации маршрутов, повышения эффективности выполнения задач. Кроме того, подчеркивается эффективность мониторинга лесных пожаров путем оснащения беспилотных летательных аппаратов сенсорными датчиками. Дана интеллектуальная система управления интегрированным программным комплексом БПЛА. Предложены методы алгоритмического шифрования надежного механизма обеспечения безопасности передачи данных ChaCha20 в управлении с помощью аудиосигнала БПЛА.

Ключевые слова: беспилотные летательные аппараты (БПЛА), сенсорные датчики, управление огнем, информационная безопасность, коммуникационная система, алгоритмы шифрования, кибербезопасность.

A.M.Moldamurat[1], D.M.Kalmanova[2], A.Baimanova*[2], Kh.Moldamurat[2], G.A.Begimova[2]

[1]LLP «Managing Company»Kazmedia ortalygy», Astana, Kazakhstan

[2]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Fire control and information protection in the communication of received signals using unmanned aerial vehicles

Abstract. This article describes the information protection of the fire monitoring and communication system by equipping unmanned aerial vehicles (UAVs) with touch sensors. Since the UAV is equipped with touch sensors, fire control provides for the transmission of signals from sensors to the center and information protection of its communication system. Effective methods of control and management of forest fires and other types of fires with an increase in risks associated with environmental disasters are shown. This makes the UAV an indispensable tool in controlling fires. However, the use of these technologies carries the risk of data loss and communication disruption. The article analyzes modern approaches to the integration of information transmission security and a sensor data management system, including encryption, authentication and protection against cyber attacks. Recommendations are given on the creation of a comprehensive protection of the communication system, which will improve the reliability and efficiency of management in a crisis. The basic principles of the UAV system functioning are described, including decision-making algorithms and coordination of actions of several unmanned aerial vehicles in one network. The methods of route optimization and improving the efficiency of tasks are considered. In addition, the effectiveness of monitoring forest fires by equipping unmanned aerial vehicles with sensor sensors is emphasized. An intelligent control system for an integrated UAV software package is given. The methods of algorithmic encryption of a reliable mechanism for ensuring the security of ChaCha20 data transmission in control using the UAV audio signal are proposed.

Keywords: unmanned aerial vehicles (UAVs), sensor sensors, fire control, information security, communication system, encryption algorithms, cybersecurity.

References

1. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – Pearson, 2017.

2. Diffie W., Martin E. New Directions in Cryptography // IEEE Transactions on Information Theory. – 1976. – T. 22, № 6. – S. 644-654.

3. Atanov S.K., Seitkulov E.N., Moldamurat Kh., Yergaliyeva B.B., Balbayev G.K., Ospanov R.M. Uyalı baylanıs zhane symsyz zhuyeler dabyldaryn intellektual'dy türde basuga arnalgan kurylgy, Patent № 8530, 2023/0753.2, 06.07.2023. – RGP «Natsional'nyy institut intellektual'noy sobstvennosti», Respublika Kazakhstan.

4. Khamis M.A., Kamel W.A. Drone Security: Issues and Challenges // International Journal of Computer Applications. – 2018. – T. 182, № 30. – S. 1-7.

5. Moldamurat Kh., Makish S.B., Atanov S.K., Bakyt M.A. Ustroystvo kriptograficheski zashchishchennogo upravleniya mobil'nym robotom, Patent № 9067, 2024/0437.2, 26.04.2024. – RGP «Natsional'nyy institut intellektual'noy sobstvennosti».

6. Cheng G., Kwan C. Security Problems in UAV Applications // IEEE Communications Magazine. – 2015. – T. 53, № 4. – S. 54-59.

7. Moldamurat K., Seitkulov Y., Atanov S., Bakyt M., Yergaliyeva B. Enhancing Cryptographic Protection, Authentication, and Authorization in Cellular Networks: A Comprehensive Research Study // International Journal of Electrical and Computer Engineering. – 2024. – T. 14, № 1. – S. 479-487.

8. Almaganbet T.Sh., Askarbek M.A., Atanova A.A. Garysh salasinda kriptokorgau zhüyesin paidalanudyn manyzdilygy men erekshelikteri // XIX Mezhdunarodnaya nauchnaya konferentsiya studentov i molodykh uchenykh «Gylym zhaNe bilim – 2024». – ISBN 978-601-7697-07-5. – S. 203-211.

9. Zhang X., Wang Y. Multisensor Data Fusion for Fire Detection in Urban Fire Control using UAVs // Sensors. – 2019. – T. 19, № 4. – S. 936.

10. Pimentel A.R., et al. Aerial Detection of Fires Using Drones and Infrared Cameras: A Case Study // Journal of Fire Sciences. – 2016. – T. 34, № 2. – S. 145-161.

11. Anderson K., Gaston G. Lightweight Drones: Development of an Unmanned Aerial Vehicle (UAV) for Environmental Monitoring // Remote Sensing. – 2013. – T. 5, № 7. – S. 3279-3297.

12. Lague D., Bouchard M. UAVs for Monitoring and Assessing the Impact of Forest Fires // Remote Sensing. – 2017. – T. 9, № 1. – S. 50.

13. Bakyt M., Moldamurat K., Konyrkhanova A., Maidanov A., Satybaldina D. Integration of Cryptography and Navigation Systems in Unmanned Military Mobile Robots: A Review of Current Trends and Perspectives // CEUR Workshop Proceedings. – 2024. – T. 3680.

14. Sigh V., Raghunathan M. Security and Privacy Issues in Drone Technology: A Survey // IEEE Access. – 2020. – T. 8. – S. 23249-23272.

15. Zhang Q., et al. Survey on Firewall Technologies in UAV Networks // Future Generation Computer Systems. – 2020. – T. 105. – S. 375-385.

Авторлар туралы мәлімет:

А.М.Молдамурат – «Ғарыштық техника және технологиялар» мамандығы бойынша техникалық ғылымдар магистрі, «Қазмедиа орталығы» басқарушы компаниясының радиохабар тарату кешенінің инженер-программисті, Дінмұхамед Қонаев көшесі, 4, 010000, Астана, Қазақстан.

Д.М.Калманова – педагогика ғылымдарының кандидаты, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің «ғарыштық техника және технологиялар» кафедрасының доцент м.а., Сәтбаев көшесі, 2, 010000, Астана, Қазақстан.

Х.Молдамурат – техника ғылымдарының кандидаты, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің «ғарыштық техника және технологиялар» кафедрасының ассистент профессоры, Сәтбаев көшесі, 2, 010000, Астана, Қазақстан.

А.Байманова – хат-хабар үшін автор, Л.Н.Гумилев атындағы Еуразия ұлттық университетінің «Ғарыштық техника және технологиялар» мамандығы бойынша техника ғылымдарының магистрі, Астана қаласы Сарыарқа ауданы әкімі аппаратының автоматтандыру инженері, Сарыарқа даңғылы 13, 010000, Астана, Қазақстан.

Г.А.Бегимова – түркология кафедрасының доценті, филология ғылымдарының кандидаты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтбаева көшесі, 2, 010000, Астана, Қазақстан.

А.М.Молдамурат – магистр технических наук по специальности «Космическая техника и технологии», инженер-программист радиовещательного комплекса управляющей компании ТОО «КазМедиа орталығы», ул. Динмухамед Кунаев, 4, 010000, Астана, Казахстан.

Д.М.Калманова – автор корреспонденции, кандидат педагогических наук, и.о. доцент кафедры «Космическая техника и технологии», Евразийский национальный университет им. Л.Н. Гумилева, ул. Сатпаева, 2, 010000, Астана, Казахстан.

Х.Молдамурат – кандидат технических наук, ассистент профессор кафедры «Космическая техника и технологии» Евразийского национального университета им. Л.Н. Гумилева, ул. Сатпаева, 2, 010000, Астана, Казахстан.

А.Байманова – автор корреспонденции, магистр технических наук по специальности «Космическая техника и технологии» Евразийского национального университета им. Л.Н. Гумилева, инженер по автоматизации аппарата акима района Сарыарка города Астана, проспект Сарыарка 13, 010000, Астана, Казахстан.

Г.А.Бегимова – доцент кафедры тюркологии, кандидат филологических наук Евразийского национального университета имени Л.Н. Гумилева, ул. Сатпаева, 2, 010000, Астана, Казахстан.

A.M. Moldamurat – Master of Technical Sciences in «Space Engineering and Technology» a software engineer for the broadcasting complex of the management company «KazMedia Center» located at 4 Dinmukhammed Kunayev Street, 010000, Astana, Kazakhstan.

D.M. Kalmanova – Candidate of Pedagogical Sciences and Acting Associate Professor of the Department of «Space Engineering and Technology» at the Eurasian National University named after L.N. Gumilyov, located at 2 Satpayev Street, 010000, Astana, Kazakhstan.

Kh. Moldamurat – Candidate of Technical Sciences and an Assistant Professor of the Department of «Space Engineering and Technology» at the Eurasian National University named after L.N. Gumilyov, located at 2 Satpayev Street, 010000, Astana, Kazakhstan.

A. Baimanova – Master of Technical Sciences in «Space Engineering and Technology» from the Eurasian National University named after L.N. Gumilyov, and an automation engineer for the Akimat of the Saryarka district of Astana, located at 13 Saryarka Avenue, 010000, Astana, Kazakhstan.

G.A. Begimova – Associate Professor of the Department of Turkology and a Candidate of Philological Sciences at the Eurasian National University named after L.N. Gumilyov, located at 2 Satpayev Street, 010000, Astana, Kazakhstan.