КІБЕРНЕТИКА та КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 623.7:004.05Ф6 DOI:10.34229/2707-451X.22.2.8

М.І. ОГУРЦОВ, В.Ю. КОРОЛЬОВ, О.М. ХОДЗІНСЬКИЙ

ДО ПРОБЛЕМ ПОКРАЩЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ДЕРЖАВНОГО ВПІЗНАВАННЯ

Розглянуто вимоги до систем впізнавання повітряних об'єктів цивільного і військового застосування. Описано недоліки і переваги існуючої системи державного впізнавання об'єктів (СДВО). Подано рекомендації щодо усунення недоліків СДВО. Подано опис лабораторного стенду для дослідження алгоритмів СДВО з резервними каналами на базі пакетної передачі зашифрованих пакетів даних програмно-керованими радіостанціями.

***Ключові слова**: державне впізнавання, ідентифікація об'єктів, криптографія, резервні канали.*

Вступ. 2022 рік показав нагальну необхідність вдосконалення існуючих систем впізнавання об'єктів типу «свій-чужий», що викликана зростанням кількості технічних засобів (особливо – безпілотних) на полі бою. Так в Україні оголошено створення армії дронів [1]. Ця концепція передбачає, комплексну закупівлю, ремонт та заміну безпілотних авіаційних комплексів (БпАК). На першому етапі виконання програми буде зібрано 200 БпАК тактичного рівня для повітряної розвідки. На другому – що кожен підрозділ Збройних Сил України (ЗСУ) буде мати власний розвідувальний БпАК.

Слід зважати, що це призведе до багатократного збільшення одночасної кількості безпілотні літальні апарати (БПЛА), що можуть знаходитись у повітрі в зоні контролю повітряного простору. Бо окрім тактичних розвідувальних БПЛА підрозділів ЗСУ в повітрі можуть знаходитись стратегічні розвідувальні пілотні та безпілотні засоби, ударні безпілотні комплекси, крилаті та балістичні ракети – і все це разом зі звичними літаками та гвинтокрилами. А потім це число ще слід у всякому разі подвоїти – щоб урахувати відповідну кількість ворожих цілей, що знаходяться у повітрі.

Таке різке зростання кількості об'єктів, що водночас приймають участь у бойових діях у повітрі, потребує вдосконалення систем впізнавання військових об'єктів як за якісними, так і за кількісними показниками. Це вимагає розробки відповідних алгоритмів ідентифікації об'єктів типу «свій-чужий» нового покоління. Подібні алгоритми можуть ґрунтуватись на різних методах захисту інформації, зокрема, на симетричних і асиметричних криптографічних алгоритмах та інших методах криптографії [2, 3].

Але слід ураховувати, що асиметричні алгоритми працюють значно повільніше за симетричні (навіть у випадку використання ключів меншої довжини, достатньої лише для криптографії поля бою [4]). А оскільки ситуація у повітряному просторі поля бою змінюється особливо динамічно, то розпізнавання об'єктів має відбуватись максимально швидко – тому

застосування симетричних криптографічних алгоритмів отримує значну перевагу за рахунок вищої швидкодії.

Також слід вважати на корінні відмінності у вимогах до систем впізнавання повітряних об'єктів цивільного та військового застосування. При їх визначенні використаємо означення «легітимний повітряний об'єкт» – це повітряний об'єкт, що має право знаходитись у даному повітряному просторі, має працюючий відповідач системи державного впізнавання та видає правильні відповіді на запити від центру впізнавання.

Основні питання, що розглядаються у даній роботі:

– основні вимоги до системи державного впізнавання об'єктів (СДВО) як до системи обробки, передачі, захисту інформації та ідентифікації об'єктів на базі методів криптографії та комп'ютерної безпеки;

– виділення спільних та відмінних рис для цивільних та військових систем впізнавання;

– визначення переваг і недоліків існуючої СДВО;

– формулювання рекомендацій для усунення недоліків існуючої СДВО;

– розробка стенда та апаратно-програмної основи для дослідження алгоритмів СДВО з резервними каналами.

Визначимо **основні вимоги до систем впізнавання повітряних об'єктів цивільного застосування** (відповідачі для системи управління повітряним рухом):

1) **максимальна сумісність**. Система впізнавання має визначати належність кожного повітряного об'єкту, включаючи літаки та гвинтокрили великих та малих авіакомпаній з усього світу та приватних власників;

2) **підтримка великої кількості об'єктів**. У зв'язку зі зростанням кількості авіаперевезень, системи впізнавання повітряних об'єктів (особливо при застосуванні у великих аеропортах) повинні підтримувати опрацювання одночасно великої кількості повітряних цілей;

3) **підтримка застарілих комплексів впізнавання**. Система має підтримувати випадки, коли запит надходить на об'єкт, що містить застарілу систему впізнавання – щоб мати можливість коректно обробити отриману відповідь та визначити належність об'єкту;

4) **підтримка альтернативних шляхів впізнавання**. У випадку, якщо автоматичне впізнавання повітряного об'єкту не вдалось, диспетчер повинен мати можливість дізнатись належність повітряного об'єкту альтернативним шляхом. Зазвичай це відбувається запитом з використанням радіозв'язку;

5) **підтримка альтернативних методів введення даних**. У випадку, якщо приналежність об'єкту була визначена альтернативним шляхом, диспетчер повинен мати можливість ввести отриману інформацію у систему вручну, щоб іншім диспетчерам не потрібно було ще раз використовувати альтернативні шляхи впізнавання.

Тепер розглянемо системи впізнавання типу «свій-чужий» **для військових застосувань**. Основним принципом роботи будь-якої сучасної системи державного впізнавання, що використовується у військових застосуваннях, є обробка вхідного запиту за формулою, що є криптографічним секретом та регулярно (наприклад, кожні 24 години) змінюється. На відміну від цивільних систем, для них виділено наступні **основні вимоги**:

1) **максимально висока швидкодія процесу впізнавання**. Оскільки ситуація на полі бою змінюється дуже швидко, а для повітряного бою це твердження є ще актуальнішим, то будь-яка затримка у процесі впізнавання може призводити до втрат, аж до людських втрат. Так, наприклад, для зенітно-ракетних комплексів час перебування цілі в зоні ураження зазвичай не перевищує декілька десятків секунд;

2) **захищеність від помилково-позитивних спрацювань**. Для цивільного застосування випадки видачі одного повітряного об'єкта за інший є теоретично малоймовірними (та без залучення у військових застосуваннях ще не зустрічались) – оскільки у випадку виявлення підлогу власник повітряного об'єкту не зможе уникнути відповідальності і втратить дуже велику кількість грошей на штрафах та судових позовах. З іншого боку, у військових застосуваннях, оскільки супротивник максимально зацікавлений у тому, щоб видати власні повітряні об'єкти за наші і готовий прикладати для цього практично необмежені час та ресурси, а результатом помилково-позитивного спрацювання системи впізнавання повітряних об'єктів можуть стати руйнування та людські жертви, то захист від подібного має бути найвищім пріоритетом системи державного впізнавання;

3) **захищеність від імітації роботи відповідача легітимного повітряного об'єкта**. Оскільки весь обмін інформацією у системі державного впізнавання «свій-чужий» виконується через радіоефір, то цілком можлива ситуація, коли всі дані, що циркулюють між повітряним об'єктом, що має право знаходитись у повітряному просторі та дає правильну відповідь на запит «свій-чужий», та центром впізнавання може бути перехоплений супротивником. Після цього супротивник може спробувати просто повторювати ті самі відповіді на запити від центру впізнавання, або спробувати змінювати їх потрібним чином, щоб зімітувати легітимний повітряний об'єкт. Саме тому система державного впізнавання повинна бути надійно захищена від атак такого типу;

4) **підтримка великої кількості об'єктів**. Як вже зазначалось вище, система державного впізнавання військового призначення має підтримувати одночасне розпізнавання великої кількості різнотипних повітряних об'єктів, щоб вчасно визначати приналежність літаків, гелікоптерів, БПЛА та їх роїв та крилатих ракет;

5) **захищеність від випадків втрати легітимного повітряного об'єкта**. Ця вимога має бути врахована на випадок, якщо легітимний повітряний об'єкт був збитий над територією, або іншим шляхом потрапила до рук ворога. Якщо подібного захисту немає, то вищеописана ситуація призведе до компрометації усієї системи державного впізнавання та необхідності її заміни на усіх легітимних повітряних об'єктах. Подібне вже траплялось, наприклад, у Радянському Союзі [5]. Таким чином, секретним має бути не сам відповідач а інформація в ньому, причому вона повинна мати можливість легкої заміни;

6) **ротація секретної частини**. Щоб запобігти можливості викрадення секретної частини відповідей, для системи державного впізнавання військового застосування ротація секретної частини має відбуватись на постійній основі. Зазвичай рекомендованим значенням є зміна секретної відповіді кожного дня. Ця вимога перетинається з попередньою вимогою та доповнює її;

7) **захищеність від помилково-негативного спрацювання для запобігання дружнього вогню**. Як вже зазначалось вище, обмін запитами і відповідями з повітряним об'єктом відбувається через радіоефір. У випадку військових дій такий обмін зазвичай ускладнений (наприклад, використанням засобів радіоелектронної боротьби (РЕБ), як дружніх, так і ворожих). Але комплекс впізнавання «свій-чужий» має працювати максимально надійно, щоб запобігти нерозпізнавання правильної відповіді легітимного повітряного об'єкта (наприклад, через ненадходження або часткове надходження правильної відповіді до центру впізнавання через дію засобів РЕБ). Ця проблема – дуже актуальна, щоб запобігти спрацюванню, наприклад, засобів протиповітряної оборони (ППО) по дружнім цілям (так званий «дружній вогонь»). Проблема може здаватись надуманою – але, наприклад, війська США під час операції «Буря в пустелі» в 1991 році понесли 23% втрат саме від «дружнього вогню» [6];

8) **захищеність від атак типу «man in the middle»**. Розглянемо таку ситуацію: легітимний повітряний об'єкт знаходиться над територією, контрольованою супротивником. Центр розпізнавання знаходиться далеко від нього, і прямий зв'язок між ними на даний момент відсутній (напри-

клад, через дію засобів РЕБ). Десь на території між легітимним повітряним об'єктом та центром впізнавання знаходяться наземний комплекс супротивника, оснащений системою радіозв'язку, та повітряний об'єкт супротивника. Комплекс впізнавання надсилає запит впізнавання повітряному об'єкту супротивника. Той ретранслює запит наземному комплексу, який передає його легітимному повітряному об'єкту. Легітимний об'єкт надсилає відповідь, яка знов таки ретранслюється з ворожого повітряного об'єкта до центру впізнавання. В результаті центр впізнавання вважатиме ворожий повітряний об'єкт – легітимним;

9) **гнучка можливість інтеграції з системою впізнавання блоку NATO**. Оскільки Україна тримає курс на євроатлантичну інтеграцію та швидкими темпами переходить на стандарти NATO, то в майбутньому виникне необхідність інтеграції військової системи впізнавання об'єктів з відповідною системою країн NATO – для виконання міжнародних навчань та операцій;

10) **наявність можливостей суто вітчизняного виробництва та супроводу системи впізнавання об'єктів**. Якщо для цивільних систем можлива закупка системи в цілому або її складових за кордоном – то для державної системи впізнавання об'єктів такий підхід неприпустимий через підвищення ризиків витоку інформації потенційним супротивникам;

11) **захищеність від засобів РЕБ**. Ця вимога пов'язана з декількома іншими і визначає, що комплекс впізнавання об'єктів «свій-чужий» має працювати та визначати належність об'єктів навіть у випадку активного застосування засобів радіоелектронної боротьби;

12) **підтримка декількох режимів впізнавання**. Зазвичай при впізнаванні військових об'єктів використовують запити типу «Де ти?» та «Хто ти?», підтримка яких має бути забезпечена. Крім того, застосовують режими звичайного та контрольного впізнавання (для виявлення ворожих повітряних об'єктів, що використовує завади проти засобів впізнавання);

13) **автоматичне блокування пуску засобів ураження типу «земля-повітря» та «повітря-повітря»** по об'єктам, що підтверджує свою легітимність правильною відповіддю на запит.

Як бачимо, єдиним перетином у вимогах до систем впізнавання об'єктів цивільного та військового призначень є лише підтримка великої кількості об'єктів.

Визначення переваг та недоліків існуючої системи державного впізнавання об'єктів. На сьогоднішній день для криптографічного захисту інформації у системі державного впізнавання типу «свій-чужий» використовується апаратно-програмний комплекс "Пароль-М", який є модифікацією радянської системи, розробленої у 80-х роках минулого століття та сам був розроблений на заміну давно застарілому комплексу «Кремній-2 (2М)», що підтримувала лише 10 запитувачів та 10 відповідачів одночасно.

Технічні можливості комплексу "Пароль" передбачають одночасне розпізнавання до 110 запитувачів і 110 відповідачів [7]. При цьому аналогічна система в країнах блоку NATO – MarkXII виконує у номінальному режимі 400 опитувань в секунду [8].

Переваги системи державного впізнавання, що використовується в Україні на даний час:

1) наявність режиму імітостійкого впізнавання;
2) наявність режиму гарантованого впізнавання;
3) здатність виконувати процедуру впізнавання навіть в умовах застосування високоінтенсивних завад;
4) наявність індивідуальних кодів для впізнавання за принципом «Хто ти?»;
5) захист від прийому відповідей по бокових пелюстках діаграми спрямованості;
6) застосування високого частотного діапазону;
7) рознесення частот запитів та відповідей [5].

Після відповіді на кожен запит від запитувача передавач відповідача на певний визначений у параметрах системи час вимикається за допомогою замикаючого пристрою [9]. Цим запобігають

відповіді на радіосигнали, які відбиті від прилеглих місцевих предметів чи отримані сигналів по боковим пелюсткам діаграми направленості. При дуже великій частоті запитів ситуація може досягти рівня, при якому порушується нормальна робота системи. Для запобігання цьому використовується автоматичне обмеження максимального числа відповідей. Для цього інтегрують дешифровані сигнали запиту, а напруга отриманого сигналу застосовується для регулювання швидкості роботи каналу формування відповідей. Обмеження частоти відповідей дозволяє також запобігти тепловому перевантаженню генератора відповідача при великому числі запитів [7, 9].

Засоби керування високоточними засобами ураження повітряних об'єктів окрім радіотехнічних способів підвищення точності впізнавання об'єктів [7, 9] мають забезпечувати:

1) зменшення кількості об'єктів у промені радіолокатора;
2) звуження діаграми спрямованості радіолокатора;
3) запобігання прийому відбитих сигналів за бічними пелюстками від радіолокатора багатоканальних приймачів;
4) когерентний прийом і передачу сигналів впізнавання.

Можливе також додаткове застосування технології розпізнавання військових об'єктів [9], техніки та особового складу супротивника для віднесення до "своїх" або "чужих" на базі розпізнавання образів.

Застосування роїв БПЛА у збройних конфліктах на Близькому сході, оснащення засобами впізнавання новітніх екіпірувань солдат, високоінтенсивні конфлікти з одночасним застосуванням пілотованої, безпілотної авіації та крилатих ракет показує, що впізнавання 110 об'єктів у зоні відповідальності військового підрозділу на сьогоднішній день є недостатнім. Цю проблему можна вирішити розробкою нових систем впізнавання об'єктів типу «запит-відповідь», які відповідатимуть сучасному рівню вимог.

Таким чином, **недоліки системи державного впізнавання, що використовується в Україні на даний час**:

1) підтримка недостатньої кількості об'єктів розпізнавання;
2) недостатній радіоелектронний захист процесу впізнавання;
3) недостатня імітостійкість – ймовірність імітації сигналу супротивником складає цілих 0.5% [7] – тобто у випадку надсилання рою з 200 ворожих БПЛА один з них зможе видати себе за свого;
4) відсутність взаємодії з усіма типами наземних засобів ураження (броньована наземна техніка, ручні засоби протиповітряної оборони і т. д.) для запобігання дружнього вогню;
5) відсутність можливості інтеграції з системою впізнавання «свій-чужий» блоку НАТО;
6) недостатня кількість кодів індивідуального впізнавання для запитів типу «Хто ти?»;
7) висока ймовірність виявлення та перехоплення сигналів впізнавання;
8) робота системи практично в усіх деталях відома супротивнику (спеціалістам з Російської Федерації).

В країнах NATO питанню впізнавання об'єктів на полі бою на сьогоднішній день присвячений великий обсяг робіт [10–12]. Серед напрямів розвитку так званої Battlefield Combat Identification System (BCIS) слід виділити:

- впізнавання, що базується на засобах автоматичної радіопередачі даних про свої війська (Radio Based Combat Identification – RBCI);
- впізнавання за допомогою радіоміток (Radio Frequency Identification tags – RF tags);
- впізнавання цілей на полі бою (застосування Battlefield Target Identification Device – BTID).

RBCI, яку також називають Battlefield Force Tracking System (BFTS), або Blu-Force Tracking (BFT) System, будується на мережецентричних принципах. Кожен дружній об'єкт військової техніки (ОВТ), обладнаний системою, кожні 5 хвилин передає дані про своє місцезнаходження засо-

бами супутникового зв'язку або в мережі радіозв'язку в діапазоні ультракоротких хвиль. В активному режимі запитувач надсилає загальний запит з координатами – а відповідач порівнює отримані координати зі своїми, і якщо вони співпадають – надсилає відповідь. Всі дані у безпровідних каналах зв'язку шифруються.

Перевагою такого підходу є можливість впізнавання об'єктів поза зоною прямої видимості. Недоліками є необхідність використання складної системи ретрансляторів на полі бою, швидке старіння даних для об'єктів, що швидко рухаються, високий вплив засобів РЕБ та висока вартість системи.

Впізнавання за допомогою радіоміток (RF tags) також базується на принципі «запит-відповідь», як і для цивільних міток, що застосовують, наприклад, у складській справі, відповідь формується шляхом модуляції вхідного запита. Застосовують активні (аналог BTID), напівактивні (мають власне джерело живлення) та пасивні (живляться енергією запиту від запитувача) мітки. Дальність впізнавання по активній чи напівактивній мітці може досягати 40 км [10]. Фактично, радіомітки є єдиним на сьогоднішній день потенційно застосовним методом впізнавання для визначення приналежності окремих військовослужбовців чи малих їх підрозділів на полі бою. А в зв'язку з їх малими розмірами та вимогами до живлення вони є потенційно застосовні і для БпАК.

Системи BTID призначені для впізнавання об'єкта військової техніки (ОВТ) у форматі «друг-невідомий». Сутність його не відрізняється від загального впізнавання системи IFF (Identification Friend or Foe – упізнавання «друг-ворог») Mk XII. Термін «друг-невідомий» був введений у військову практику з оглядом на те, що об'єкт упізнавання, який не відповідає на запит, не обов'язково є ворожим об'єктом [10]. Системи BTID також працюють за принципом «запит-відповідь», сигнали зашифровані, та, для зменшення ймовірності перехоплення, є широкополосні.

Подамо **результати** статті у формі низки рекомендацій.

Рекомендації щодо усунення виявлених недоліків системи державного впізнавання та підвищення рівня її надійності:

1) заміна поточної системи державного впізнавання на більш сучасну, що підтримуватиме більш сучасні криптографічні алгоритми та більшу кількість об'єктів розпізнавання;

2) підтримка ліній впізнавання різних напрямів, включаючи «Земля – БПЛА», «Літак – Танк», «Літак – БПЛА» та інших;

3) додавання підтримки стандарту NATO – STANAG 4579, що був прийнятий у 2001 році, та інших;

4) додавання підтримки впізнавання за допомогою радіоміток (RF tags);

5) застосування сигналів з широким спектром для зменшення ймовірності виявлення та перехоплення, а також низки сигнально-кодових конструкцій та робочої сітки частот.

Створення макету системи державного впізнавання

Практика боротьби з ворожими авіацією, БПЛА та ракетами показала, що багато літальних засобів супротивника були збиті ручними пусковими установками, які не передбачають використання систем державного впізнавання. Оскільки супротивник використовує літальні апарати радянської доби або їх модернізовані варіанти зі дуже схожими силуетами, досить багато часто атакованими бувають і власні літальні апарати. Тому запропоновано використовувати низку резервних каналів для державного впізнавання та створити малогабаритний пристрій, який можна встановити на переносні ракетні комплекси.

Як лабораторний макет було використано дві пари програмно-керованих радіостанцій Ettus B200 і HackRF One, які виконували функції основного і резервного каналів передачі даних. Тобто основний канал [13, 14] може використовувати широкосмугові сигнали у діапазоні надвисоких частот в якому працюють радіолокатори зенітних ракетних систем, а резервний канал в ультракороткохвильовому діапазоні можуть використовувати запитувачі переносних зенітно-ракетних ком-

плексів. Крім різних робочих частот основний і резервний канали використовували різні типи кодування: ортогональне мультиплексування з частотним поділом і квадратурну амплітудну маніпуляцію. Обидва канали використовують однаковий тип шифрування пакетів даних. На рисунку показано фрагменти лабораторних стендів для демонстрації роботи системи державного впізнавання з резервними каналами.

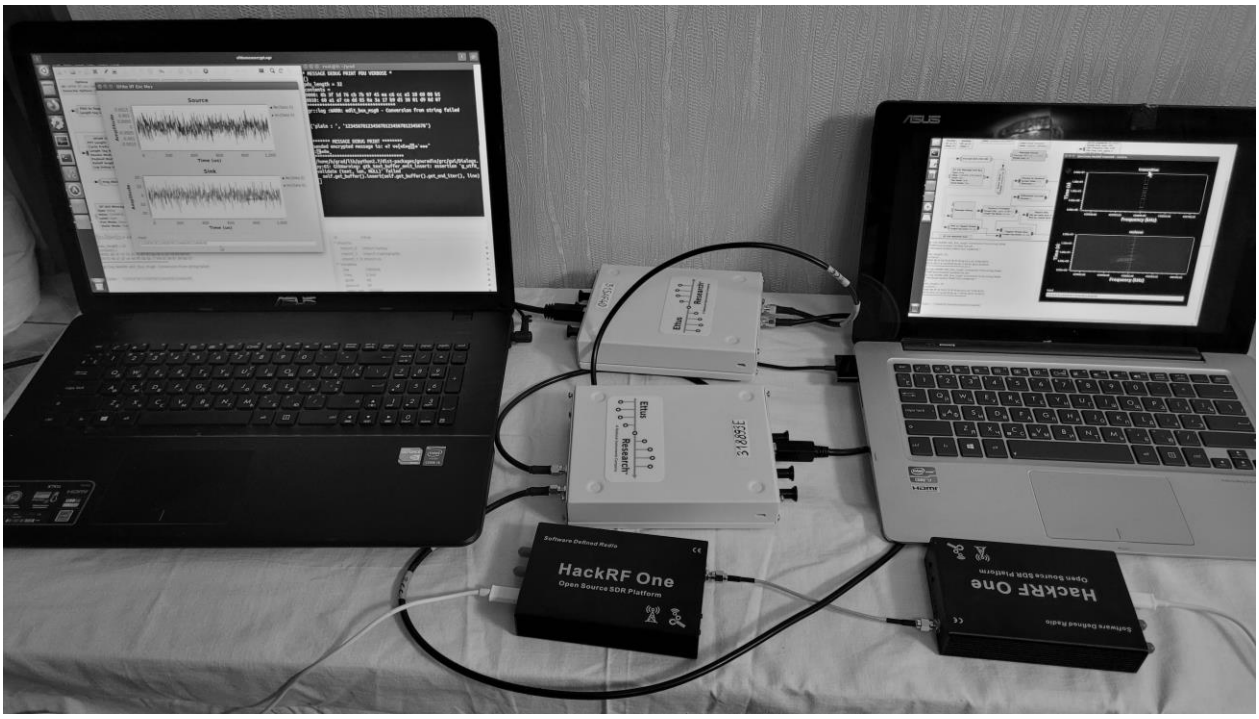

РИСУНОК. Лабораторний стенд для дослідження роботи системи державного впізнавання з резервними каналами

Виконані експерименти показали стабільну роботу системи у лабораторних умовах для зашифрованих AES-256 32-байтних пакетів даних, що є основою для подальших дослідно-конструкторських робіт [13].

Висновки. Використання супротивником аналогічних ОВТ ускладнює візуальне визначення їх державної приналежності за принципом "свій-чужий" та призводить до "дружнього вогню". Використання низки різноманітних засобів ППО, які передають союзники, ставить проблему подальшої інтеграції таких засобів у ППО України, що потребує, зокрема, розробки відповідних пристроїв державного впізнавання. Такі пристрої можуть використовувати різні типи частотних діапазонів та сигнально-кодових конструкцій, а їх розробка ґрунтуватиметься на різних вимогах до масогабаритних характеристик та потужності передавача сигналу державного впізнавання. Використання багатьох різнотипних систем та вимоги до інтегрованості систем державного впізнавання з системами блоку NATO та США поставить питання про надійність системи в цілому.

Підвищення надійності систем державного впізнавання та зв’язку ґрунтується на створенні низки резервних каналів передачі даних. Такі резервні канали мають використовувати різні робочі частоти та відмінні типи частотної маніпуляції цифрових радіосигналів, щоб збільшити стійкість системи спеціального зв’язку до заглушення станціями радіоелектронної боротьби.

Зважаючи на обмеженість фінансових ресурсів в Україні можна запропонувати використовувати більш дорогі радіостанції для виконання державного впізнавання на основних частотах, і дешевші радіостанції для державного впізнавання на резервних частотах.

Запропоновані результати можна також використовувати для побудови захищених систем зв'язку, дистанційного керування роботами, безпілотними літальними апаратами, безпілотними наземними роботами. Напрацьовані результати можна перенести на програмовану логічну інтегральну схему та використовувати у військовій справі, якщо це мікросхема і виконання виробу відповідатимуть стандартам експлуатації у відповідних родах військ ЗСУ.

Список літератури

1. Генштаб ЗСУ, Мінцифри та UNITED24 збирають «Армію дронів», Міністерство цифрової трансформації України, https://www.kmu.gov.ua/news/genshtab-zsu-mincifri-ta-united24-zbirayut-armiyu-droniv (звернення: 01.07.2022)
2. Rudinskas D., Goraj Z., Stankūnas J. Security Analysis Of UAV Radio Communication System. *Aviation*. 2009. **13** (4). P. 116–121. https://doi.org/10.3846/1648-7788.2009.13.116-121
3. Огурцов М.І. Розробка протоколу захисту даних для спеціальних мереж. *Математика та комп'ютерне моделювання.* 2019. **19**. С. 108–113. http://dspace.nbuv.gov.ua/handle/123456789/168579
4. Matt B. J. Lightweight and Survivable Key Management for Army Battlefield Networks. Internal Publication, Network Associates Laboratories. 2003. http://projects.mindtel.com/2005/SDSU.Geol600.Sensor_Networks/sensornets.refs/2003. ASC. Army Studies Conference/OA05 Lightweight and Survivable Key Management for Army Battlefield Networks.pdf (звернення: 25.07.2022)
5. Ермак С.Н., Касанин О.А., Хожевец С.Н. Устройство и эксплуатация наземных средств системы государственного опознавания. Минск: БГУИР, 2017. 230 с.
6. Waterman D. L. Fratricide: Incorporating DESERT STORM Lessons Learned. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.828.2521&rep=rep1&type=pdf (звернення 25.07.2022)
7. Закревский А. Свой — чужой. https://dou.ua/forums/topic/10097/ (звернення: 25.07.2022)
8. STANAG 4193. Technical Characteristics Of The IFF Mk XIIA System. NATO, 2016. p. 45. https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/volume2/ch03s03.html (звернення 25.07.2022)
9. Канащенков А.И., Меркулов В.И. Радиолокационные системы многофункциональных самолетов. М.: Радиотехника, 2006. 656 с.
10. Камалтинов Г. Г. Впізнавання об'єктів на полі бою. Аналіз світового досвіду. *Озброєння та військова техніка*. 2016. **4**. С. 22–26. http://nbuv.gov.ua/UJRN/ovt_2016_4_5
11. Rohan P., Gangopadhyay A., Erbacher A. R., Busartet C. Camouflaged object detection system at the edge. *Automatic Target Recognition* XXXII. Vol. 12096. SPIE, 2022. https://doi.org/10.1117/12.2618869
12. Nolan P., Hamilton S. IFF using Beamforming in Telemetry Beacons. *2021 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*, IEEE, 2021. P. 1–5. https://doi.org/10.1109/WNYISPW53194.2021.9661287
13. Корольов В.Ю., Огурцов М.І., Кочубінський А.І. Ідентифікація технічних об'єктів в спеціальних мережах за принципом "свій–чужий". *Control Systems and Computers*. 2021. **4**. С. 3–12 https://doi.org/10.15407/csc.2021.04.003
14. Корольов В.Ю., Огурцов М.І., Ходзінський О.М. Багаторівневе державне впізнавання об'єктів та аналіз застосовності пост-квантових криптографічних алгоритмів для захисту інформації. *Cybernetics and Computer Technologies*. 2020. **3**. С. 74–84. https://doi.org/10.34229/2707-451X.20.3.7

Одержано 29.08.2022

Огурцов Максим Ігорович,
науковий співробітник Інституту кібернетики імені В.М. Глушкова НАН України, Київ,
https://orcid.org/0000-0002-6167-5111

Корольов Вячеслав Юрійович,
кандидат технічних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ,
https://orcid.org/0000-0003-1143-5846

Ходзінський Олександр Миколайович,
кандидат фізико-математичних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ.
https://orcid.org/0000-0003-4574-3628
okhodz@gmail.com

UDC 623.7:004.056

Maxim Ogurtsov, Vyacheslav Korolyov, Oleksandr Khodzinskyi *

To the Problems of the National State Recognition System Improving

V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv
* *Correspondence: okhodz@gmail.com*

Introduction. A rapid increase in the number of objects that simultaneously take part in combat operations in the air requires improvement of systems for recognizing military objects both in terms of qualitative and quantitative indicators. This requires the development of appropriate algorithms for identifying new-generation "friend-foe" objects. Such algorithms can be based on various methods of information security, in particular symmetric and asymmetric cryptographic algorithms and other methods of cryptography.

The purpose of the article is to survey modern systems of state recognition of objects (SSRO), identify their shortcomings and provide recommendations for their elimination.

Results. The requirements for SSRO as a system for processing, transmitting, securing information and identifying objects based on cryptography and computer security methods are defined. Common and distinctive features for civil and military identification systems are highlighted. The advantages and disadvantages of the existing SSRO are shown. Recommendations are formulated to address the shortcomings of the existing SSRO. An example of a stand and a hardware and software basis for studying SSRO algorithms with backup channels is given.

Conclusions. Eliminating the shortcomings of the SSRO and improving the level of its reliability will require the implementation of the following organizational and technical measures.

1. Replacing the current state recognition system with a more modern one, which will support more modern cryptographic algorithms and a larger number of recognition objects. Adding support for radio tag recognition (RF tags).

2. Support for recognition lines in various directions, including "ground – UAV", "plane – tank", "plane – UAV" and others. Adding support for the NATO standard – STANAG 4579, adopted in 2001, and others.

3. Using of broad-spectrum signals to reduce the probability of detection and interception, as well as a number of signal-code structures and a working frequency grid.

Keywords: Friend-or-Foe, object identification, cryptography, backup channels.