DOI https://doi.org/10.15407/csc.2021.04.003
УДК 004.056

В.Ю. КОРОЛЬОВ, кандидат технічних наук, старший науковий співробітник,
Інститут кібернетики ім. В.М. Глушкова НАН України,
03187, м. Київ, просп. Академіка Глушкова, 40, Україна,
koro1oyv@i.ua

М.І. ОГУРЦОВ, науковий співробітник, Інститут кібернетики ім. В.М. Глушкова
НАН України, 03187, м. Київ, просп. Академіка Глушкова, 40, Україна,
maksymogurtsov@gmail.com

А.І. КОЧУБІНСЬКИЙ, кандидат фіз.-мат. наук, старший науковий співробітник,
Інститут кібернетики ім. В.М. Глушкова НАН України,
03187, м. Київ, просп. Академіка Глушкова, 40, Україна,
ks0610@ukr.net

ІДЕНТИФІКАЦІЯ ТЕХНІЧНИХ ОБ'ЄКТІВ У СПЕЦІАЛЬНИХ МЕРЕЖАХ ЗА ПРИНЦИПОМ "СВІЙ–ЧУЖИЙ"

Зростання кількості дистанційно-керованих об'єктів військової техніки потребує перегляду методів і алгоритмів державного впізнавання (ДВ), що використовуються. У роботі запропоновано новий алгоритм ДВ об'єктів та ідентифікації військовослужбовців за допомогою симетричних криптографічних алгоритмів та використання захищеного протоколу обміну інформацією, отриманою з мережі Збройних Сил України. Такий підхід дає змогу потенційно збільшити продуктивність і якість роботи системи впізнавання.

Ключові слова: *державне впізнавання, дистанційна ідентифікація об'єктів, спеціальні мережі, «свій-чужий», криптографія.*

Вступ

Впровадження мережевих технологій управління військовими підрозділами та масове застосування безпілотних літальних апаратів (БПЛА), а також наземних і підводних роботів під час бойових операцій висуває нові вимоги до продуктивності систем державного впізнавання (ДВ) [1–5] й алгоритмів дистанційної ідентифікації технічних об'єктів [3]. Сьогодні у Збройних Силах України (ЗСУ) для ДВ об'єктів військової техніки (ОВТ) за принципом «свій-чужий» використовується комплекс «Пароль-М», який є модифікацією радянської системи, розробленої у 80-х роках минулого століття. Комплекс «Пароль» передбачає, що у тактичній зоні може бути до 110 запитувачів і 110 відповідачів [4], аналогічна система в країнах блоку *NATO — Mark*XII виконує в номінальному режимі 400 опитувань за секунду [5]. Застосування роїв БПЛА у збройних конфліктах на Близькому Сході, оснащення засобами впізнавання новітніх екіпірувань військовослужбовців показує, що впізнавання 110 об'єктів у зоні відповідальності військового підрозділу може виявитись недостатнім. Цю проблему можна розв'язати розробкою нових систем кодування та шифрування сигналів ДВ ОВТ, які відповідатимуть сучасному рівню вимог.

Зростання кількості рухомих роботизованих систем [6–10] у сучасних збройних конфліктах потребує вдосконалення систем впізнавання

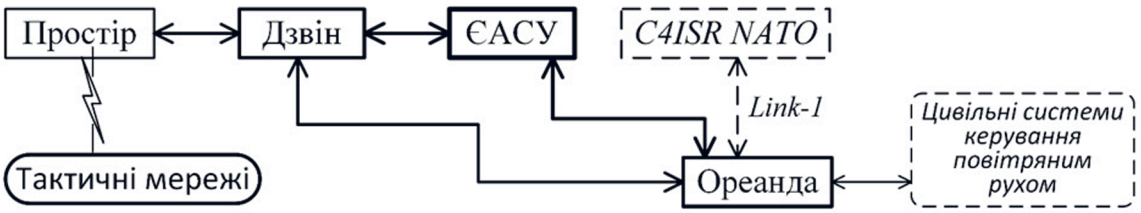

Рис. 1. Багаторівнева організація обміну даними в АСУ ЗСУ [15]

військових об'єктів за якісними та кількісними показниками. Широке застосування БПЛА та їхніх роїв [6–10] у різних сферах [1], зокрема, в новітніх гібридних конфліктах, потребує розробки мережевих алгоритмів ДВ та передачі інформації [8–16], що можуть ґрунтуватися на методах передачі та захисту інформації у спеціальних мережах, а саме симетричних й асиметричних алгоритмах шифрування даних [10, 13] та інших методах криптографії [11, 12, 14].

Вторинні джерела ідентифікаційних даних для системи ДВ ОВТ

Концепція мережо-центричної війни передбачає територіальне розподілення військової техніки та пунктів керування для уникнення одночасного знищення їх, але при цьому не повинна втрачатися керованість підрозділами та можливість координації вогню з різних місць по цілях, що забезпечується багатократним резервуванням захищених мережевих каналів зв'язку та передачі даних. Системи ДВ [1, 2, 15] є складовою частиною оборонних автоматизованих систем (рис. 1), які керують військовою авіацією, протиповітряною обороною, взаємодіють із цивільними системами керування повітряним рухом, військовими системами радіотехнічної та авіаційної розвідки. Для захисту передачі інформації на всіх рівнях та всіх подібних системах застосовуються симетричні й асиметричні криптографічні алгоритми.

Іншою проблемою є «дружній вогонь», тобто обстріли своїх підрозділів, які було помилково ідентифіковано як ворожі. У сучасних військових конфліктах, у яких брали участь країни-члени *NATO* проти суттєво слабкішого супротивника, такі втрати ОВТ склали до 80 відсотків [1]. Це стало однією з причин появи у новітніх комплексах екіпірування військовослужбовців підсистем, що дають змогу визначити на полі бою «свого» або «чужого» солдата і щодо окремих військових, і щодо тактичних груп. Індустріально розвинуті країни мають власні системи ДВ: США (*Ratheon*), Франція (*Thales*), Іспанія (*AMIGO*), Росія («Страж», КРЭТ) [1].

Способи ідентифікації об'єктів для систем ДВ ОВТ

Сучасні комплекси розпізнавання цілей для військових літальних апаратів [1, 3] складаються з декількох систем, до переліку яких входить система ДВ, вони об'єднуються системою підтримки прийняття рішень пілота для застосування засобів ураження. Алгоритми ДВ ОВТ ЗСУ, які використовуються системами автоматичного впізнавання за принципом «свій-чужий», з погляду безпеки інформації є алгоритмами зі змінними параметрами для ідентифікації технічних об'єктів на базі паролів із ротацією їх у часі [11–17]. Тобто задача полягає в розробці алгоритмів ідентифікації користувачів технічної системи з урахуванням особливостей для системи ДВ ОВТ на базі алгоритмів криптографії.

Відомі такі способи ідентифікації, засновані на різних типах криптографічних перетворень [11, 14, 16]:

1. Ідентифікація на основі алгоритмів симетричного шифрування.

2. Ідентифікація на основі кодів аутентифікації повідомлень; по суті це алгоритми хешування із секретним початковим станом, які є варіантом способу 1.

3. Ідентифікація на основі алгоритмів асиметричного шифрування.

4. Ідентифікація на основі алгоритмів обчислення та перевірки цифрового підпису.

5. Комбінація перерахованих методів у різних поєднаннях.

Очевидно, що кожен спосіб має свої переваги та недоліки. Наприклад, спосіб 1 є найпростішим і найшвидшим, він дає змогу створювати системи реального масштабу часу для військових систем. Його недолік полягає в необхідності генерації та розподілу секретних ключів. Способи 3 і 4 передбачають виконання операцій у групі точок еліптичної кривої, доволі витратних з погляду обчислювальних ресурсів, а використання способів ідентифікації на основі криптографії з відкритим ключем (способи 3 і 4) потребує розгортання інфраструктури підтримки цієї криптографії, до якої входять генератори пар ключів, центр сертифікації відкритих ключів, сервер перевірки стану сертифікатів відкритих ключів, аутентифікація сертифікатів тощо.

Таку серверну інфраструктуру вже частково розгорнуто в мережах спеціального зв'язку ЗСУ для систем типу «Дзвін АС» та «Ореанда ПС», але її взаємодію з мережевою системою ідентифікації технічних об'єктів потрібно перевірити на реальній обчислювальної системі щодо швидкості виконання такого алгоритму ідентифікації. Використання алгоритму в реальних умовах вимагатиме його ускладнення для протистояння специфічним для цих умов загрозам. Розроблена в Інституті кібернетики імені В.М. Глушкова НАН України криптографічна бібліотека [17] дає змогу реалізувати будь-який із перерахованих способів, зокрема, за допомогою повноцінного центру сертифікації ключів у відповідності до ДСТУ 4145-2002. Мати власний мобільний центр сертифікації ключів потрібно в разі втрати зв'язку із центром керування або погіршення зв'язку внаслідок застосування засобів РЕБ.

Постановка проблеми

ЗСУ потребують розробки нової власної системи ДВ ОВТ, яка забезпечуватиме надійну ідентифікацію об'єктів, матиме високу продуктивність обробки даних із можливістю подальшого масштабування системи. Така система має забезпечувати захист інформації та захист від дії засобів РЕБ, має інтегруватися у спеціальні мережі ЗСУ, використовувати дані від цивільних систем керування рухом тощо.

У статті уточнено перелік вимог до сучасних систем ДВ, розглянуто питання інтеграції систем ДВ ОВТ у спеціальні мережі ЗСУ. Далі викладено новий алгоритм захисту інформації системи ДВ та подано приклад технічної реалізації алгоритму ідентифікації за принципом «свій-чужий» на базі програмно-керованих радіостанцій.

Алгоритм ДВ ОВТ

Суть роботи алгоритмів ДВ — це обробка кодів запитів і відповідей ОВТ, які зашифровані симетричним криптографічним алгоритмом. Такий підхід обрано тому, що потрібна максимальна продуктивність системи впізнавання, а обмін публічними ключами за асиметричною системою може не спрацювати в умовах дії природніх шумів або навмисних завад, створених комплексами РЕБ супротивника.

У групи ОВТ може бути короткотерміновий спільний ключ, яким зашифровуються та розшифровуються пакети даних ДВ, або в кожного ОВТ може бути свій сесійний ключ шифрування даних ДВ та окремий ідентифікатор, за яким станція ППО або ОВТ знаходить цей ключ у таблиці та розшифровує пакети даних ДВ.

Іншим рекомендованим підходом є використання асиметричного криптографічного алгоритму лише для шифрування ключа симетричного алгоритму для його відправлення до передачі сигналів запиту/відповіді [11–16]. У цьому разі можливість розшифрувати та використати ключ симетричного алгоритму автоматично означає наявність ключа асиметричного алгоритму.

За аналогією із цивільними системами керування повітряним рухом, у відповідь військовий технічний об'єкт може надати не тільки

свій ідентифікатор, а й дані про координати, тип літака тощо [4, 5], що може бути додатково використано для запобігання підміні сигналу відповіді та перевірці справжності отриманого коду.

ОВТ, включений у підсистеми Єдиної Автоматизованої Системи Управління ЗСУ [15, 16], може також використовувати інформацію від цивільних систем для верифікації даних, отриманих через спеціальні мережі [6–10], що застосовують симетричні й асиметричні криптографічні алгоритми захисту інформації для забезпечення багаторівневого ДВ ОВТ.

Алгоритм захисту інформації системи державного впізнавання

Розгляньмо один із можливих варіантів роботи системи ДВ — з використанням розробленого криптографічного алгоритму.

1. Перед виконанням задач ДВ у центрі керування повітряним рухом заздалегідь генерується відкритий довготерміновий ключ K для асиметричного алгоритму шифрування та копіюється на кожний ОВТ. Він зберігається й на кожному ОВТ, й у центрі керування повітряним рухом для подальшого тривалого використання. Пара до цього відкритого ключа — закритий ключ K_3 — зберігається лише в центрі керування повітряним рухом.

2. Кожному ОВТ призначається свій унікальний ідентифікатор I_i, що зберігається в його довготерміновій пам'яті. База всіх ідентифікаторів I також зберігається у центрі керування повітряним рухом.

3. Для кожного ОВТ генерується унікальна пара ключів Q_o та Q_z. Відкритий ключ Q_o зберігається в центрі керування повітряним рухом, а закритий Q_z — в пам'яті ОВТ.

4. За необхідності виконання процедури впізнавання центр керування повітряним рухом надсилає невпізнаному літальному об'єкту (НЛО) відкритий (не зашифрований) запит на впізнавання B_i, що містить позначку дати та часу (включно із секундами) T_i.

5. НЛО, отримавши запит на впізнавання B_i, шифрує отриману позначку дати та часу T_i закритим ключем Q_z. Після цього він шифрує свій ідентифікатор I_i й попередньо зашифровану позначку дати та часу довготерміновим ключем K. Далі НЛО передає зашифровану відповідь до центру керування повітряним рухом. Зашифрована відповідь НЛО на запит впізнавання має вигляд: $[I_i, [T_i] Q_z] K$.

6. Центр керування повітряним рухом отримує зашифровану відповідь від НЛО. Він розшифровує її довготерміновим закритим ключем K_3 — й отримує ідентифікатор об'єкта I_i. Далі у своїй базі даних центр керування знаходить відповідний об'єкту I_i відкритий ключ Q_o, та використовує його для розшифрування позначки дати та часу T_i. Якщо розшифрована позначка дати та часу збігається з тією, що була відправлена НЛО на кроці 4, то це підтверджує, що НЛО є тим літальним апаратом, за який він себе видає (апарат з ідентифікатором I_i або «свій»).

7. За необхідності повторити процедуру впізнавання кроки 4–6 виконуються знову.

У тому разі, якщо інформація про захоплені супротивником/втрачені/знищені ОВТ буде вчасно оновлюватися в базі даних центру керування повітряним рухом, то така система ДВ забезпечуватиме достатню стійкість і надійність впізнавання. Інакше супротивник, захопивши ОВТ, може просто переставити систему відповіді на запит впізнавання на один зі своїх літальних апаратів. У цьому разі вкрадена система впізнавання даватиме правильні відповіді на запити від центру керування повітряним рухом.

За необхідності виконувати захищений обмін даними після завершення процедури впізнавання, в алгоритм слід внести такі зміни:

– На кроці 5 НЛО генерує сеансовий ключ для симетричного криптографічного алгоритму KS_i. Далі НЛО шифрує ключем Q_z не лише позначку дати та часу T_i, й ключ KS_i. Вигляд відповіді на запит від системи впізнавання в цьому разі описується залежністю:

$$[I_i, [T_i, KS_i] Q_z] K.$$

– На кроці 6 центр керування повітряним рухом розшифровує відповідь послідовно ключами K_3 та Q_o й отримує ключ KS_i, який засто-

совує для подальшого обміну даними з ОВТ, використовуючи симетричний алгоритм шифрування.

Після відповіді на кожен запит передавач відповідача на деякий час вимикається за допомогою вимикального пристрою [3, 4]. Цим запобігають відповіді на радіосигнали, відбиті від прилеглих місцевих предметів тоді, коли частоти запиту та відповіді збігаються, а коди є подібними. За дуже великої частоти запитів кількість відповідей кожному запитувачу зменшується й може досягти рівня, при якому порушується нормальна робота системи. Для запобігання цьому у відповідачах застосовується автоматичне обмеження максимальної кількості відповідей. Воно здійснюється шляхом інтегрування дешифрованих сигналів запиту та використання напруги одержаного сигналу для регулювання швидкості роботи каналу формування відповідей. Пристрій обмеження частоти відповідей дає змогу також запобігти тепловому перевантаженню генератора відповідача, коли надходить велика кількість запитів [3, 4].

Новітні засоби керування високоточною зброєю, окрім радіотехнічних способів підвищення точності впізнавання об'єктів [3], мають забезпечувати: зменшення кількості об'єктів у промені радіолокатора, звуження діаграми спрямованості радіолокатора, запобігання прийому відбитих сигналів за бічними пелюстками від радіолокатора багатоканальних приймачів, когерентний прийом і передачу сигналів впізнавання. Вони мають використовувати також технології розпізнавання ОВТ [3], техніки та солдат супротивника для віднесення об'єкта до «своїх» або «чужих» на базі розпізнавання образів

Сучасні комплекси розпізнавання цілей для військових літальних апаратів (ЛА) [3] складаються з декількох систем, до переліку яких входить і система ДВ, що об'єднуються системою підтримки прийняття рішень пілотом для застосування засобів ураження. Алгоритми ДВ ОВТ ЗСУ, які використовуються системами автоматичного впізнавання за принципом «свій-чужий», з точки зору безпеки інформації є алгоритмами зі змінними параметрами для ідентифікації технічних об'єктів на базі паролів з ротацією їх у часі [11–16].

Розвиток алгоритмів, що використовуються у системах ДВ ОВТ [3, 4], є подібним до еволюції систем автентифікації користувачів комп'ютерних систем і мереж [13], де відбувся поступовий перехід від однофакторних систем ідентифікації до багатофакторних систем автентифікації з резервними варіантами авторизації доступу, що застосовують асиметричні криптографічні алгоритми для надання дистанційного доступу до інформаційних сервісів у мережі Інтернет.

Системи радіолокаційного впізнавання

Інформація про державну приналежність використовується на всіх етапах організації авіаційного руху та інших застосувань і тому є вкрай важливою. Сучасна система ДВ має відповідати низці загальних вимог:

– мати високу перешкодозахищеність і для запитного каналу, і для каналів відповіді;

– мати достатню стійкість до імітації сигналів відповіді ОВТ;

– мати високу пропускну здатність (надійно працювати за наявності в тактичній зоні великої кількості запитувачів і відповідачів);

– мати достатні точні характеристики, що забезпечується роздільною здатністю за дальністю та кутовими координатами;

– мати високу експлуатаційну надійність і малий час відновлення;

– характеристики системи мають бути узгоджені з характеристиками РЛС, з якими вона пов'язана. При цьому максимальна дальність розпізнавання має бути більшою або дорівнювати максимальній дальності виявлення РЛС.

Структура системи ДВ на базі програмно-керованих радіостанцій

У загальнішому випадку (рис. 2) на стороні наземного пункту керування (НПК) використовують мережу багатоканальних дистанційно-

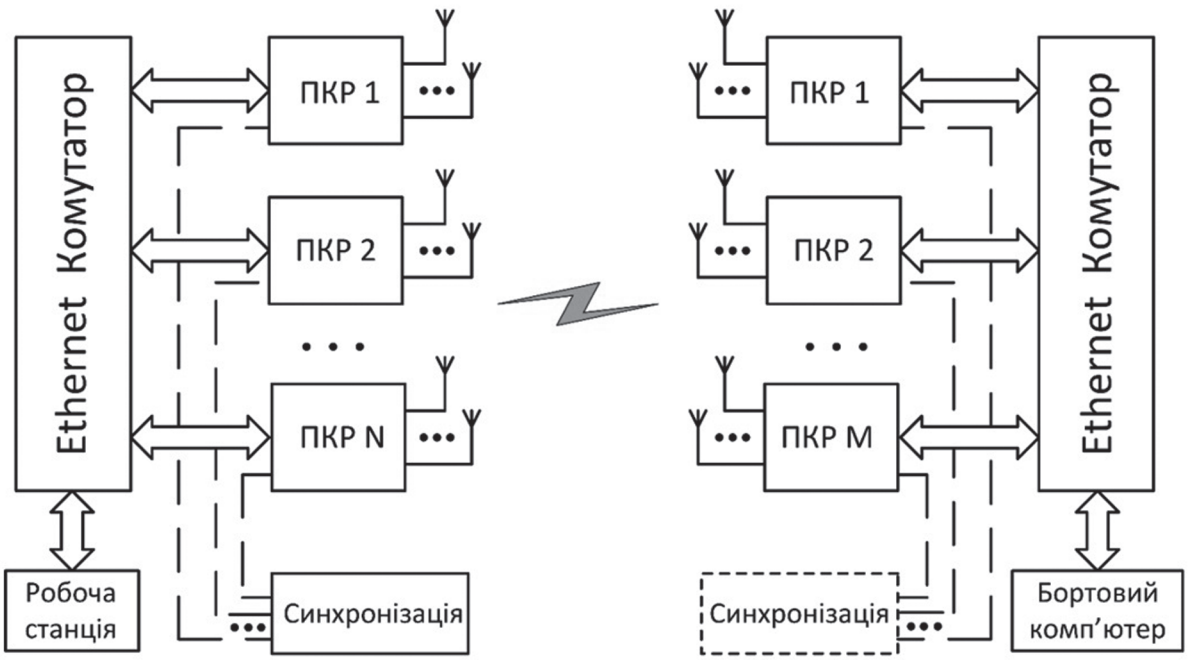

Рис. 2. Структурна схема передачі даних між НПК та БПЛА

керованих радіостанцій [1, 3, 4, 6, 11, 16], які обмінюються даними з робочою станцією через *Ethernet*-комутатор. Для покращення використання робочого простору їх можуть встановлювати у стійку за принципом серверних.

Щоб забезпечити стабільність частоти, застосовують три види синхронізації за часом:

– від робочої станції;

– від системи глобального позиціонування (якщо вона незаглушена);

– від термостабілізованого генератора опорної частоти для загальної синхронізації всіх програмно-керованих радіостанцій від окремого багатоканального джерела високостабільної частоти.

Оскільки ЛА або БПЛА має обмежені корисне навантаження і об'єм для розміщення електронних засобів, на ньому можна розмістити меншу кількість програмно-керованих радіостанцій (ПКР) та засобів синхронізації робочої частоти, ніж на НПК. З урахуванням масогабаритних обмежень БПЛА пропонується для бортових систем використовувати як основний третій вид синхронізації, а перший і другий використовувати як допоміжні.

Радіолінія системи ДВ ґрунтується на пакетному радіозв'язку та складається із цифрового приймача та передавача, які реалізують захищений канал передачі запитів і відповідей. Для моделювання каналу захищеної передачі даних пропонується використати програмне середовище *GNURadio*, у якому побудовано два *OFDM* (*Orthogonal Frequency-Division Multiplexing* — мультиплексування з ортогональним частотним розділом каналів), радіомодеми з 32 піднесучими частотами та смугою пропускання 1 МГц (рис. 3). На стороні запитувача вхідні дані запиту зашифровуються, перетворюються на формат, зручний для пакетного радіозв'язку, і транслюються на відповідач. На стороні відповідача виконується обернене перетворення інформації та формується в аналогічний спосіб відповідь, яка надсилається запитувачу.

На рис. 4 наведено скріншот екрану розробленого спеціалізованого програмного комплексу під час роботи алгоритму ДВ. Рядок запиту «12345678123456781234567 8» довжиною 32 байти шифрується алгоритмом *AES*-256 (режим *CBC*) за допомогою бібліотеки *Cryptography*

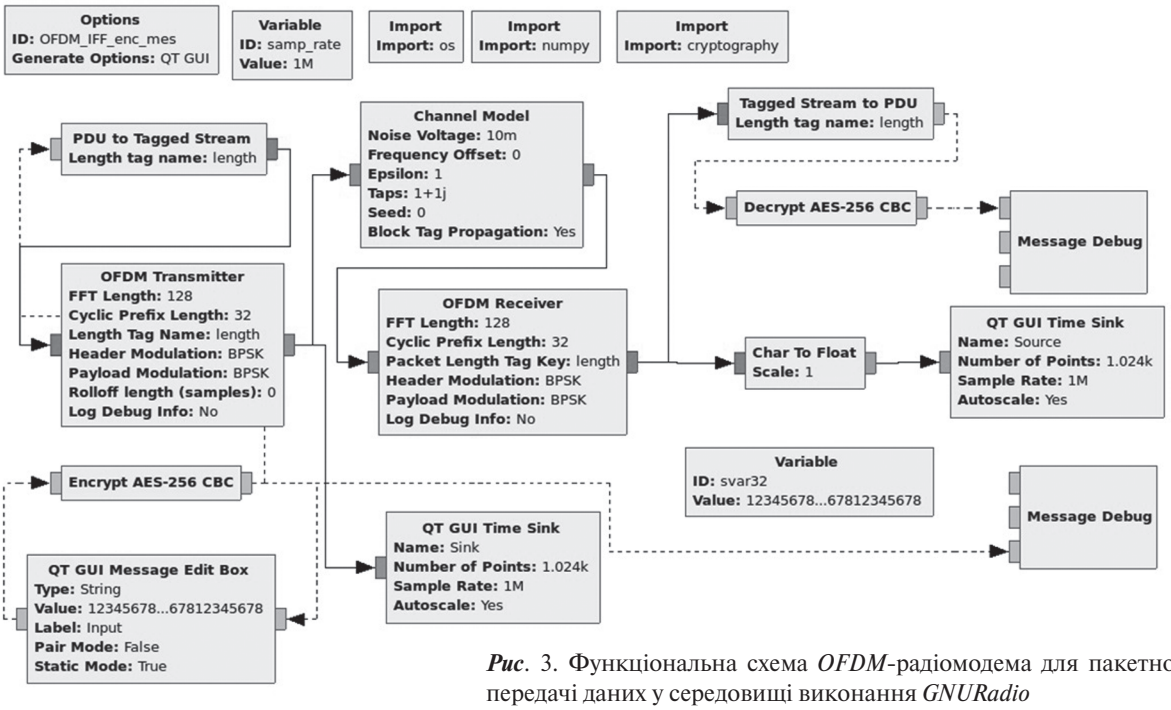

Рис. 3. Функціональна схема *OFDM*-радіомодема для пакетної передачі даних у середовищі виконання *GNURadio*

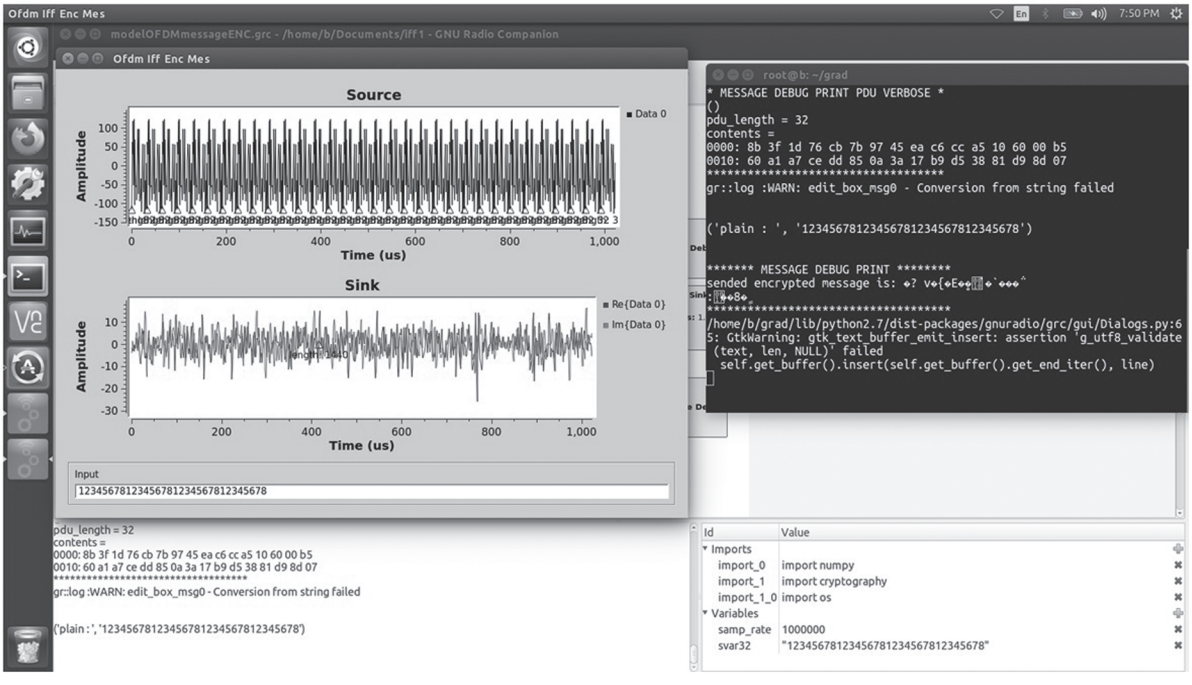

Рис. 4. Скріншот під час відправлення зашифрованого пакету даних і його розшифрування

для мови програмування *Python* та транслюється радіомодемом (запитувач). Другий радіомодем (відповідач) отримує пакет даних та розшифровує його.

Отже, побудовано обчислювальну систему, що симулює роботу *OFDM* модему для комп'ютерного моделювання процесів передачі та прийому даних і тестування алгоритмів ДВ. Запропонована система дозволяє виконувати захищену передачу пакетів даних в асинхронному режимі.

Отримані результати можна також використати у системах передачі інформації та керування технічними об'єктами.

Висновки

Підвищення ефективності, надійності та стійкості систем захисту інформації нині є першочерговими завданнями для багатьох організацій та галузей у будь-якій країні світу. У системах захисту спеціальних мереж істотну роль відведено криптографічним засобам захисту, які вважаються одними з надійніших та найефективніших.

У статті запропоновано новий багаторівневий алгоритм ДВ, який дає змогу виконувати надійну автоматизовану ідентифікацію об'єктів, масштабувати систему, обмінюватися даними про потенційні цілі через захищені мережі. Це дасть змогу покращити розуміння ситуації на полі бою (*dominant battle space awareness*) у реальному масштабі часу за допомогою використання інформації з доступних джерел. Розроблений алгоритм ДВ об'єктів є краще захищеним порівняно з наявними алгоритмами й орієнтованим на використання сучасних бортових комп'ютерів та програмованих радіомодемів.

Розроблений алгоритм ДВ базується на криптографічних бібліотеках, розроблених в ІК НАНУ і забезпечує підвищення рівня захищеності зв'язку та команд керування при передачі між групами БПЛА і НПК на основі алгоритму *AES* в режимі ланцюгування шифроблоків та з використанням випадкового вектора ініціалізації.

Розроблено комп'ютерну модель *OFDM* модему для тестування алгоритмів ДВ. Запропонована модель дає змогу виконувати симуляцію захищеної передачі пакетів, даних в асинхронному режимі. Отримані результати можна також використати для систем передачі інформації та керування технічними об'єктами.

Напрямом подальших досліджень є використання стрибкоподібної зміни частоти для задач ДВ та поєднання системи з чарунковою мережею, яка імітуватиме спеціальну систему зв'язку ЗСУ (Оренда та система керування вищого ієрархічного рівня) й отримання даних із цивільних мереж про ситуацію навколо станції конкретного НПК.

ЛІТЕРАТУРА

1. *Камалтинов Г. Г., Кукобко С. В., Маляренко О. С., Кісєль П. І.* Впізнавання об'єктів на полі бою. Аналіз світового досвіду. *Озброєння та військова техніка*. 2016. 4. С. 22–26. DOI: https://doi.org/10.34169/2414-0651.2016.4(12).22-26.
2. ДСТУ 4550:2006. Система державного впізнавання об'єктів. Впізнавання радіолокаційне. Терміни та визначення понять. [Чинний від 2007-08-01]. Вид. офіц. Київ : Держспоживстандарт України, 2007. 21 с.
3. *Канащенков А. И., Меркулов В. И.* Радиолокационные системы многофункциональных самолетов. М. : Радиотехника. 2006. 656 с.
4. *Ермак С. Н., Касанин С. Н., Хожевец О. А.* Устройство и эксплуатация наземных средств системы государственного опознавания : учебное пособие. Минск : БГУ-ИР, 2017. 230 с. URL: https://libeldoc.bsuir.by/bitstream/123456789/13383/2/Ermak_2017.pdf.
5. STANAG 4193. Technical Characteristics Of The IFF Mk XIIA System. NATO. 2016. P. 45.
6. *Корольов В. Ю.* Маршрутизація ланки крилатих ракет багаторазового використання. УСиМ. 2019. 2. С. 16–24. DOI: https://doi.org/10.15407/usim.2019.02.016.
7. *Корольов В. Ю., Огурцов М. І.* Транспортно-комунікаційна задача для груп безпілотних апаратів. *Математичні машини і системи*. 2017. 1. С. 82–89. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/117508/07-Korolev.pdf?sequence=1.
8. *Корольов В. Ю., Поліновський В. В., Огурцов М. І.* Моделювання мереж зв'язку рухомих дистанційно керованих систем на базі HLA. *Вісник Хмельницького національного університету*. 2017. 1 (245). С. 160–165. URL: https://

icyb180.org.ua/wp-content/uploads/2017/07/modelyuvannya-merezh-zvyazku-ruhomih-distantsiyno-kerovanih-sistem-na-bazi-hla.pdf.

9. *Корольов В. Ю., Ходзінський О. М.* Тополого-комбінаторна модель побудови мереж для транспортних засобів. *Комп'ютерна математика*. 2018. 1. С. 61–67. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/161850/08-Korolev.pdf?sequence=1.
10. *Rudinskas D., Goraj Z., Stank nas J*. Security Analysis of UAV Radio Communication System. *Aviation*. 2009. 13 (4). P. 116–121. URL: https://www.tandfonline.com/doi/pdf/10.3846/1648-7788.2009.13.116-121.
11. *Gupta R., Kumari A., Tanwar S., Kumar N*. Blockchain-Envisioned Softwarized Multi-Swarming UAVs to Tackle COVID-I9 Situations. *IEEE Network*. 2021. 35 (2). P. 160–167.
12. *Огурцов М. І.* Розробка протоколу захищеного обміну даними для спеціальних мереж. *Математичне та комп'ютерне моделювання*. Серія: Технічні науки : зб. наук. праць. Кам'янець-Подільський національний університет ім. Івана Огієнка, 2019. 19. С. 108–113.
13. *Alia M. A., Tamimi A. A., Al-Allaf O. N*. Cryptography based authentication methods. *WCECS 2014* : Proceedings of the World Congress on Engineering and Computer Sci-ence, 22-24 October, 2014, San Francisco, USA. 2014. 1. P. 199-204. URL: http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp199-204.pdf.
14. *Огурцов М. І., Корольов В. Ю.* Криптографічний алгоритм державного впізнавання об'єктів. *Створення та модернізація озброєння і військової техніки в сучасних умовах* : зб. матеріалів XX наук.-техн. конф., 3-4 вер. 2020 р. Чернігів : ДНДІ ВС ОВТ, 2020. С. 186–187.
15. З*аболоцький В.* Цифровий вимір ЗСУ. За яких умов це можливо? *Оборонно-промисловий кур'єр*. URL: http://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/ (дата звернення: 13.10.2020).
16. *Корольов В. Ю., Огурцов М. І., Ходзінський О. М.* Багаторівневе державне впізнавання об'єктів та аналіз застосовності пост-квантових криптографічних алгоритмів для захисту інформації. *Кібернетика та комп'ютерні технології*. 2020. 3. С. 74–84. DOI: https://doi.org/10.34229/2707-451X.20.3.7.
17. Авторське право і суміжні права. Державна служба інтелектуальної власності. Офіційний бюлетень № 36. 2015. С. 35–36. URL: https://me.gov.ua/Files/GetFile?lang=uk-UA&fileId=792a0cdf-d138-4256-911e-7e3dec55f78d (дата звернення: 06.01.2021).

Надійшла 18.05.2021

REFERENCES

1. *Kamaltinov G. G., Kukobko S. V., Malyarenko O. S., Kisel P. I.*, 2016. "Identification of objects on the battlefield. International experience analysis", Weapons and military equipment, 4, pp. 22–26. DOI: 10.34169/2414-0651.2016.4(12).22-26. (In Ukrainian).
2. DSTU 4550: 2006. System of state recognition of objects. Radar recognition. Terms and definitions. [Effective from 2007-08-01]. Kind. ofits. Derzhspozhyvstandart Ukraine, Kyiv, 2007, pp. 21. (In Ukrainian).
3. *Kanashchenkov A. I., Merkulov V. I.,* 2006. Radar systems of multifunctional aircraft, Radio engineering, Moscow, 656 p. [online] Available at: <https://libeldoc.bsuir.by/bitstream/123456789/13383/2/Ermak_2017.pdf>. (In Russian).
4. *Ermak S. N., Kasanin S. N., Khozhevets O. A.*, 2017. Device and operation of ground means of the system of state identification, textbook, BGUIR, Minsk, 230 p. [online] Available at: <https://libeldoc.bsuir.by/bitstream/123456789/13383/2/Ermak_2017.pdf>. (In Russian).
5. STANAG 4193. Technical Characteristics Of The IFF Mk XIIA System. NATO, 2016, pp. 45.
6. *Korolyov V. Yu.*, 2019. "Routing for a swam cruise rockets of multiple use", Control systems and Computers, 2, pp. 16–24. DOI: 10.15407/usim.2019.02.016. (In Ukrainian).
7. *Korolyov V. Yu., Ogurtsov M. I.*, 2017. "Transport and communication problem for groups of drones", Mathematical machines and systems, 1, pp. 82–89. [online] Available at: <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/117508/07-Korolev.pdf?sequence=1>. (In Ukrainian).
8. *Korolyov V. Yu., Polinovsky V. V., Ogurtsov M. I.*, 2017. "Modeling of communication networks of mobile remotely controlled systems based on HLA", Herald of Khmelnytskyi National University, 1 (245), pp. 160–165. [online] Available at: <https://icyb180.org.ua/wp-content/uploads/2017/07/modelyuvannya-merezh-zvyazku-ruhomih-distantsiyno-kerovanih-sistem-na-bazi-hla.pdf>. (In Ukrainian).
9. *Korolyov V. Yu., Khodzinsky O. M.*, 2018. "Topological-combinatorial model of network construction for vehicles", Computer mathematics, 1, pp. 61–67. [online] Available at: <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/161850/08-Korolev.pdf?sequence=1>. (In Ukrainian).
10. *Rudinskas D., Goraj Z., Stank nas J.*, 2009. "Security Analysis of UAV Radio Communication System", Aviation, 13 (4), pp. 116–121. [online] Available at: <https://www.tandfonline.com/doi/pdf/10.3846/1648-7788.2009.13.116-121>.

11. *Gupta R., Kumari A., Tanwar S., Kumar N.*, 2021. "Blockchain-Envisioned Softwarized Multi-Swarming UAVs to Tackle COVID-I9 Situations", IEEE Network, 35 (2), pp. 160–167.
12. *Ogurtsov M. I.*, 2019. "Development of a protocol for secure data exchange for special networks", Mathematical and computer modeling, Series "Technical Sciences", Proceedings, Kamyanets-Podilsky National University named after Ivan Ogienko, 19, pp. 108–113. (In Ukrainian).
13. *Alia M. A., Tamimi A. A., Al-Allaf O. N.*, 2014. "Cryptography based authentication methods", Proceedings of the World Congress on Engineering and Computer Science, 3 January 2014.
14. *Ogurtsov M. I., Korolyov V. Yu.*, 2020. "Cryptographic algorithm of state recognition of objects", Creation and modernization of armaments and military equipment in modern conditions, Proceedings of the XX scientific and technical conf., 3–4 Sept. 2020, DNDI VS OVT, Chernihiv, pp. 186–187. (In Ukrainian).
15. *Zabolotsky V.* "Digital measurement of the Armed Forces. Under what conditions is this possible?", Defense Industrial Courier. [online] Available at: <http://opk.com.ua/digital-dimension-of-the-support-of-the-conditions-this-possible/> (Last accessed: 13.10.2020). (In Ukrainian).
16. *Korolyov V. Yu., Ogurtsov M. I., Khodzinsky O. M.*, 2020. "Multilevel Identification Friend or Foe of Objects and Analysis of the Applicability of Post-Quantum Cryptograph-ic Algorithms for Information Security", Cybernetics and computer technologies, 3, pp. 74–84. DOI: 10.34229/2707-451X.20.3.7. (In Ukrainian).
17. Copyright and related rights. State Intellectual Property Service. Official Bulletin № 36. 2015. pp. 35–36. [online] Available at: <https://me.gov.ua/Files/GetFile?lang=uk-UA&fileId=792a0cdf-d138-4256-911e-7e3dec55f78d>. (Last accessed: 06.01.2021). (In Ukrainian).

Received 18.05.2021

V.Yu. Korolyov, Ph.D. Eng. Sciences, Senior Research Associate,
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine,
03187, Kiev, Glushkov Avenue, 40, Ukraine,
koro1ov@i.ua
M.I. Ogurtsov, Researcher Associate, V.M. Glushkov Institute of Cybernetics of
the NAS of Ukraine, 03187, Kiev, Glushkov Avenue, 40, Ukraine,
maksymogurtsov@gmail.com
A.I. Kochubinskyi, Ph.D (Physics and Math.), Senior Research Associate,
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine,
03187, Kiev, Glushkov Avenue, 40, Ukraine,
ks0610@ukr.net

IDENTIFICATION OF TECHNICAL OBJECTS IN THE SPECIAL NETWORKS ACCORDING TO THE PRINCIPLE OF "FRIEND OR FOE"

Introduction. In recent years, military conflicts are moving to a fundamentally new level of development, which is associated with the widespread use of geographically distributed large groups of remotely controlled robotic systems, the rapid growth of information volumes, a significant increase in the speed of its processing, instant messaging to increase situational awareness, management, rapid response, etc.

Purpose. The article is devoted to solving an urgent scientific problem — the development of an algorithm for state identification of military objects and personnel. The problems of using modern cryptographic algorithms for state identification, which use data obtained by other stations of the air defense system and radio intelligence, combined in a special network, are considered.

Results. A new encryption key exchange protocol and a rationale for choosing a cryptographic algorithm that can be used in real-time systems with low computational performance are proposed. To ensure stability to the use of electronic warfare tools, it is proposed to use software-defined radio stations based on programmable logic matrices as a hardware basis, since they allow changing the type of signal-code structures, which also applies frequency ranges without replacing radio engineering blocks.

Conclusions. The increase in the number of remotely controlled military equipment objects on the battlefield, the problem of positioning military personnel and equipping them with network communication means requires a review of the methods and algorithms used for state recognition. The paper proposes a new algorithm for state identification of objects and identification of military personnel using symmetric cryptographic algorithms and the use of a secure Protocol for exchanging information received from the network of the Armed Forces of Ukraine. This approach can potentially increase the performance and quality of the identification system.

Keywords: *remote identification of objects, special networks, identification "friend or foe", cryptography.*