конкретних визначених зразків. Методологічно і програмно вона сумісна з реалізованими в ЦНДІ ОВТ ЗС України методиками комплексної порівняльної оцінки зразків ОВТ, що враховують також військово-технічний рівень та фінансово-економічні показники зразків ОВТ.

Крім того методика дає можливість зробити порівняльну оцінку спроможностей створення даного або типового зразка ОВТ даного типажу рядом альтернативних підприємств, які готові надати необхідну інформацію щодо своєї фінансово-виробничої діяльності.

Методика визначення коефіцієнта спроможності виробництва зразків ОВТ дозволяє розробити, в рамках системи підтримки прийняття рішення, науково обґрунтовані рекомендації щодо вибору оптимального варіанту оснащення ЗС України необхідними зразками ОВТ.

УДК 004.056

КРИПТОГРАФІЧНИЙ АЛГОРИТМ ДЕРЖАВНОГО ВПІЗНАВАННЯ ОБ'ЄКТІВ

М.І. Огурцов

В.Ю. Корольов, *к.т.н., с.н.с.*

Інститут кібернетики імені В.М. Глушкова Національної академії наук України

Зростання кількості рухомих роботизованих систем у сучасних збройних конфліктах потребує вдосконалення систем розпізнавання військових об'єктів за якісними і кількісними показниками. Широке застосування безпілотних літальних апаратів (БПЛА) та їх роїв у новітніх гібридних конфліктах потребує розробки мережевих алгоритмів державного впізнавання (ДВ) та передачі інформації, що можуть ґрунтуватись на методах захисту інформації, а саме симетричних і асиметричних алгоритмах шифрування даних та інших методах криптографії. Іншою проблемою є "дружній вогонь" – обстріл з боку власних сил або союзників.

Сьогодні в 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, аналогічна система в країнах блоку NATO – MarkXII виконує в номінальному режимі 400 опитувань в секунду. Ряд індустріально розвинутих країни мають власні системи ДВ.

Сучасні комплекси розпізнавання цілей для військових літальних апаратів складаються з декількох систем, до переліку яких входить система державного впізнавання, що об'єднуються з системою підтримки прийняття рішень пілота для застосування засобів ураження. Алгоритми ДВ ОВТ ЗСУ, котрі використовуються системами автоматичного впізнавання за принципом "свій-чужий", з точки інформаційної безпеки є алгоритмами зі змінними параметрами для ідентифікації технічних об'єктів на базі паролів з ротацією їх у часі. У роботі пропонується розробити алгоритми для системи ДВ ОВТ на базі криптографічних алгоритмів.

Суть роботи алгоритмів ДВ – це обробка кодів запитів і відповідей ОВТ, які зашифровані симетричним криптографічним алгоритмом. Такий підхід обрано тому, що потрібна максимальна продуктивність такої системи, а обмін публічними ключами за асиметричною системою може не спрацювати в умовах дії природніх шумів або навмисних завад, створених комплексами радіоелектронної боротьби супротивника. Іншим рекомендованим підходом є використання асиметричного криптографічного алгоритму лише для шифрування ключа симетричного алгоритму для його відправлення до передачі сигналів запиту/відповіді. В цьому випадку можливість розшифрувати та використати ключ симетричного алгоритму автоматично означає наявність ключа асиметричного алгоритму.

По аналогії з цивільними системами керування повітряним рухом у відповідь військовий технічний об'єкт може надати не тільки свій ідентифікатор, але і дані про координати, тип літака та ін., що може бути додатково використано для запобігання підміні сигналу відповіді та перевірці справжності отриманого коду. ОВТ, включений у підсистеми Єдиної Автоматизованої Системи Управління ЗСУ, може також використовувати інформацію від цивільних систем для верифікації даних, отриманих через спеціальні мережі, що застосовують симетричні і асиметричні криптографічні алгоритми для захисту інформації для забезпечення багаторівневого ДВ ОВТ.

Алгоритм захисту інформації системи державного впізнавання.

Розглянемо один з можливих варіантів роботи системи державного впізнавання:

1) Перед виконанням задач державного впізнавання у центрі керування повітряним рухом заздалегідь генерується загальний відкритий довготерміновий ключ K для асиметричного алгоритму шифрування та копіюється на кожний військовий технічний об'єкт. Він зберігається і на кожному об'єкті, і у центрі керування повітряним рухом для подальшого тривалого використання. Пара до цього відкритого ключа – закритий ключ $K_з$ – зберігається виключно у центрі керування повітряним рухом.

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

3) Для кожного літального апарату 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 літального апарату.

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 (включаючи секунди) 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 та попередньо зашифровану позначку дати та часу довготерміновим ключем K. Після цього НЛО передає зашифровану відповідь до центру керування повітряним рухом.

6) Центр керування повітряним рухом отримує зашифровану відповідь від НЛО. Він розшифровує її довготерміновим закритим ключем $K_з$ – і отримує ідентифікатор об'єкта I_i. Далі в своїй базі даних центр керування знаходить відповідний об'єкту I_i відкритий ключ Q_o, та використовує його для розшифровки позначки дати та часу T_i. Якщо розшифрована позначка дати та часу співпадає з тою, що була відправлена НЛО на кроці 4, то це підтверджує, що НЛО – той літальний апарат, за який він себе видає (апарат з ідентифікатором I_i або "свій").

7) При необхідності повторити процедуру впізнавання кроки 4-6 повторюються.

У випадку, якщо інформація про захоплені супротивником/втрачені/знищені літальні апарати буде вчасно оновлюватись в базі даних центру керування повітряним рухом, то така система державного впізнавання забезпечуватиме достатню стійкість та надійність впізнавання. Інакше, супротивник, захопивши літальний апарат, може просто переставити систему відповіді на запит впізнавання на один зі своїх літальних апаратів. В цьому випадку система впізнавання буде давати правильні відповіді на запити від центру керування повітряним рухом, оскільки формально буде легітимною.

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

1) На кроці 5 алгоритму захисту інформації системи державного впізнавання НЛО генерує сеансовий ключ для симетричного криптографічного алгоритму KS_i. Далі НЛО шифрує ключем Q_z не лише позначку дати та часу T_i, але й ключ KS_i.

2) На кроці 6 алгоритму центр керування повітряним рухом розшифровує відповідь послідовно ключами $K_з$ та Q_o і отримує ключ KS_i, який застосовує для подальшого обміну даними з літальним апаратом, використовуючи симетричний алгоритм шифрування.

УДК 623.746-519:355.42

НАПРЯМКИ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ У СУЧАСНИХ БОЙОВИХ УМОВАХ

П.М. Онипченко, *к.пед.н., доцент*
Ю.М. Корнусь
Харківський національний університет Повітряних Сил імені Івана Кожедуба
О.О. Казіміров, *к.військ.н., доцент*
Національна академія Національної гвардії України

В тактиці застосування безпілотної авіації спостерігається перехід від поодинокого до групового застосування безпілотних авіаційних комплексів (БАК). В доповіді аналізується доцільність і технічна можливість щодо використання змішаних груп, які включають пілотовані й безпілотні літальні апарати. Крім того, розглядаються питання створення авіаційних груп, що включають до свого складу БАК різних класів, здатних автономно виконувати широке коло завдань у складних метеорологічних умовах, а також в умовах активної протидії противника. Основні фактори, що впливають на сумісне виконання завдань пілотованою та безпілотною авіацією можна поділити на організаційно-технічні, тактико-технічні, та військово-економічні.

Організаційно-технічні фактори, що впливають на сумісне виконання завдань пілотованою та безпілотною авіацією, включають:

- організацію управління безпілотною авіацією;
- характеристики систем управління БАК;
- ступень автономності виконання завдань БАК;
- раціональний розподіл завдань між пілотованою та безпілотною авіацією;
- організацію системи ППО противника.

Разом з цим при спільному використанні пілотованої й безпілотної авіації виникає ряд проблем, до основних з яких можна віднести наступні:

ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
ВИПРОБУВАНЬ І СЕРТИФІКАЦІЇ
ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

"СТВОРЕННЯ ТА МОДЕРНІЗАЦІЯ ОЗБРОЄННЯ І ВІЙСЬКОВОЇ ТЕХНІКИ В СУЧАСНИХ УМОВАХ"

Збірник
XX науково-технічної конференції

3 – 4 вересня 2020 року

м. Чернігів

**ДЕРЖАВНИЙ НАУКОВО–ДОСЛІДНИЙ ІНСТИТУТ
ВИПРОБУВАНЬ І СЕРТИФІКАЦІЇ
ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ**

“СТВОРЕННЯ ТА МОДЕРНІЗАЦІЯ ОЗБРОЄННЯ І ВІЙСЬКОВОЇ ТЕХНІКИ В СУЧАСНИХ УМОВАХ”

**Збірник
XX науково-технічної конференції**

03 – 04 вересня 2020 року

Чернігів 2020

УДК 623 (062.552)
Зб-41

Створення та модернізація озброєння і військової техніки в сучасних умовах: збірник XX науково-технічної конференції, 03-04 вересня 2020 р. / ДНДІ ВС ОВТ. – Чернігів: Видавець Брагинець О.В., 2020. – 295 с.

Збірник XX науково-технічної конференції Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки спрямований на висвітлення проблемних питань наукового та науково-технічного характеру у галузі створення, випробування, оцінки відповідності озброєння та військової техніки і пошук шляхів їх вирішення.

Збірник буде корисним для курсантів (студентів); наукових та науково-педагогічних працівників закладів вищої освіти; інженерів та наукових працівників у галузі створення, випробування та оцінки відповідності озброєння та військової техніки.

Збірник укладено з матеріалів, які були презентовані на науково-технічній конференції "Створення та модернізація озброєння і військової техніки в сучасних умовах". В доповідях розглянуті наукові та практичні аспекти з питань:

розроблення, модернізації, випробувань і експлуатації:

– комплексів озброєння і військової техніки, актуальні проблеми випробувань і сертифікації;

– засобів забезпечення десантних, спеціальних та пошуково-рятувальних операцій та комплексів бойової екіпіровки;

– засобів зовнішньо-траєкторних та бортових інформаційно-вимірювальних систем;

– систем управління авіаційним озброєнням та авіаційними засобами ураження;

– ракетних та зенітних ракетних комплексів (систем) та засобів ураження;

– артилерійського та стрілецького озброєння, боєприпасів та засобів ближнього бою;

– автоматизованих систем управління, бортового обладнання, радіотехнічних та радіолокаційних комплексів;

– безпілотних авіаційних комплексів і тренажерних систем;

- вимірювальних систем,

метрологічної експертизи та метрологічного забезпечення випробувань ОВТ.

Свідоцтво про державну реєстрацію КВ № 23996-13836Р від 19.06.2019

ВІДПОВІДАЛЬНІСТЬ ЗА ЗМІСТ ТЕЗ НЕСУТЬ АВТОРИ

ЗБІРНИК
XX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

ДЕРЖАВНОГО НАУКОВО-ДОСЛІДНОГО ІНСТИТУТУ
ВИПРОБУВАНЬ І СЕРТИФІКАЦІЇ
ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

СТВОРЕННЯ ТА МОДЕРНІЗАЦІЯ ОЗБРОЄННЯ І ВІЙСЬКОВОЇ ТЕХНІКИ В СУЧАСНИХ УМОВАХ

03 – 04 вересня 2020 року, м. Чернігів

Відповідальний за випуск збірника В.А. Дмитрієв

Комп'ютерна верстка А.Г. Павленко, О.В. Жирна

Техн. редактор Р.В. Холодний

Свідоцтво про державну реєстрацію КВ № 23996-13836Р від 19.06.2019

Підписано до друку 26.08.2020 р.
Формат 60 × 84/8. Папір офсетний. Гарнітура Times.
Умовн. друк. арк. 34,41. Обл.-вид.арк. 30,37.
Зам.№ 20100. Наклад 100 прим. Ціна договірна .

Віддруковано з готових оригінал-макетів ФОП Брагинець О.В.

Свід. про внесення до держ. реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції серія ДК, № 4879 від 07.04.2015. Виписка з єдиного держ. реєстру серія ААВ, № 257729 від 01.12.2011. Україна, 14029, м. Чернігів, вул. О. Кошового, 6, к. 15.
www://siver-druk.com.ua e-mail: siverdruk11@gmail.com