УДК 004.056.55:003.26 https://doi.org/10.35546/kntu2078-4481.2022.2.9

М. І. ОГУРЦОВ
Інститут кібернетики імені В. М. Глушкова Національної академії наук України
ORCID: 0000-0002-6167-5111

РОЗРОБКА АЛГОРИТМУ ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ ТИПУ «СВІЙ-ЧУЖИЙ» З ВИКОРИСТАННЯМ СИМЕТРИЧНОГО ШИФРУВАННЯ

Різке зростання кількості об'єктів, що водночас приймають участь в 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.

Метою дослідження стало визначення переваг та недоліків існуючої системи державного впізнавання об'єктів, розробка пропозицій щодо усунення виявлених недоліків та створення алгоритму державного впізнавання, позбавленого виявлених недоліків.

На основі визначених переваг та недоліків поточного алгоритму державного впізнавання запропоновано новий двоетапний алгоритм захисту інформації типу «запит-відповідь» для системи державного впізнавання для військових об'єктів, побудований на основі державних стандартів України, що забезпечуватиме достатню масштабованість, стійкість, надійність та багаторівневість впізнавання. Виконано аналіз розробленого алгоритму, його переваг та недоліків порівняно з алгоритмом, що застосовується на даний момент. Визначені можливі підходи до криптоаналізу запропонованого алгоритму та проаналізовано їх застосовність та ефективність.

Алгоритм може застосовуватись не тільки для ліній впізнавання «земля-літак», але й для таких, як «літак-літак», «літак-танк», «літак-корабель» та ін. (в тому числі, в зворотному напрямі), включаючи навіть «літак-піхотинець».

Розроблений алгоритм має вищу швидкодію порівняно з тим, що використовується на сьогоднішній день (особливо якщо говорити про Етап 1) та забезпечує вищий рівень надійності завдяки використанню сучасних криптографічних алгоритмів, що відповідають державним стандартам України.

Ключові слова: *ідентифікація, свій-чужий, криптографія, шифрування, впізнавання, радіомітки, криптографічний аналіз.*

M. I. OGURTSOV
V. M. Glushkov Institute of Cybernetics of National Academy of Sciences of Ukraine
ORCID: 0000-0002-6167-5111

FRIEND-OR-FOE IDENTIFICATION ALGORITHM DEVELOPMENT USING SYMMETRICAL ENCRYPTION

The sharp increase of objects number that simultaneously take part in air combat operations requires the improvement of military objects recognition systems both qualitatively and according to several indicators. This requires the development of appropriate new generation "friend-or-foe" algorithms for the objects` identification. Such algorithms can be based on various methods of information security, in particular on symmetric and asymmetric cryptographic algorithms and other cryptography methods.

The research included identification of advantages and disadvantages of the existing state "friend-or-foe" system, development of proposals to eliminate the identified shortcomings and creation of the "friend-or-foe" algorithm, which addressing identified shortcomings.

Based on the identified advantages and disadvantages of the current "friend-or-foe" recognition algorithm, a new two-stage request-response information protection algorithm is proposed for "friend-or-foe" recognition systems for military use, built based on Ukrainian state standards, which ensures sufficient scalability, stability, reliability, and multi-level recognition. An analysis of the developed algorithm, its advantages and disadvantages, and the shortcomings in comparison with the currently existing algorithm was performed. The possibilities of the approach to the proposed algorithm cryptanalysis were determined and their applicability and effectiveness were analyzed.

The algorithm can be used not only for «land-aircraft» recognition lines, but also for such lines as «aircraft-aircraft», «aircraft-tank», «aircraft-ship», etc. (plus the reverse direction), including the «infantry plane».

The developed algorithm has a higher speed in comparison with those used today (especially if compare Stage 1 algorithm) and provides higher level of reliability because of using modern cryptographic algorithms and the Ukrainian cryptographic state standards.

Key words: *identification, friend-or-foe, cryptography, encryption, recognition, radio tags, cryptographic analysis.*

Вступ

2022 рік показав нагальну необхідність вдосконалення існуючих систем впізнавання об'єктів типу «свій-чужий», що викликана зростанням кількості власних та ворожих літальних об'єктів на полі бою.

Постановка проблеми

Таке різке зростання кількості об'єктів, що водночас приймають участь в 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 [1], [2].

Але слід враховувати, що асиметричні алгоритми працюють значно повільніше за симетричні [3]. А оскільки ситуація в 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.

Аналіз останніх досліджень та публікацій

На сьогоднішній день для криптографічного захисту інформації в системі державного впізнавання типу «свій-чужий» використовується апаратно-програмний комплекс «Пароль-М» [4], 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-М», що використовується на даний момент в Україні, передбачають одночасне розпізнавання до 110 запитувачів і 110 відповідачів [4]. При цьому аналогічна система в країнах блоку NATO – MarkXII виконує в номінальному режимі 400 опитувань в секунду [5].

В країнах НАТО питанню впізнавання об'єктів на полі бою на сьогоднішній день присвячений великий обсяг робіт [6], [7], [8]. 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 мережоцентричних принципах. Кожен дружній об'єкт ОВТ, обладнаний системою, кожні 5 хвилин передає дані про своє місцезнаходження засобами супутникового зв'язку або в мережі УКХ зв'язку. 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, в складській справі, відповідь формується шляхом модуляції вхідного запита. Застосовують активні (аналог BTID), напівактивні (мають власне джерело живлення) та пасивні (живляться енергією запита від запитувача) мітки. Дальність впізнавання по активній чи напівактивній мітці може досягати 40 км [6]. 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 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 [6]. Системи BTID також працюють за принципом «запит-відповідь», сигнали зашифровані, та, для зменшення ймовірності перехоплення, широкополосні.

Формулювання мети дослідження

Метою дослідження є визначення переваг та недоліків існуючої системи державного впізнавання об'єктів, розробка пропозицій щодо усунення виявлених недоліків та створення алгоритму державного впізнавання, позбавленого виявлених недоліків.

Викладення основного матеріалу дослідження

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

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 [9].

Після відповіді на кожен запит від запитувача передавач відповідача на певний визначений у параметрах системи час вимикається за допомогою замикаючого пристрою [10]. 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 одержаного сигналу застосовується для регулювання швидкості роботи каналу формування відповідей. Обмеження частоти відповідей дозволяє також запобігти тепловому перевантаженню генератора відповідача при великому числі запитів [4], [10].

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 момент:**

1) Підтримка недостатньої кількості об'єктів розпізнавання.
2) Недостатній радіоелектронний захист процесу впізнавання.
3) Недостатня імітостійкість – ймовірність імітації сигналу супротивником складає цілих 0.5% [сч9] – 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).

Додаткові функції, які має забезпечувати система впізнавання:

1) Отримання від повітряного об'єкту додаткової інформації про його висоту.
2) Отримання від повітряного об'єкту додаткової інформації про його запаси пального (заряду акумуляторів).

Загальні принципи роботи системи ідентифікації об'єктів типу «свій-чужий» на основі державних стандартів України. Алгоритм ідентифікації об'єктів типу «свій-чужий» має бути побудований на основі державних стандартів України. По факту це має бути не один алгоритм, а сімейство алгоритмів – оскільки для лінії впізнавання, наприклад, «земля-літак» не може використовуватись той же самий алгоритм, що і для лінії «літак-танк». При цьому алгоритми повинні враховувати визначені вимоги та рекомендації, подані в попередньому підрозділі.

Окремо слід виділити алгоритм та процедуру генерації випадкових ключів, який також має бути заснований на державних стандартах України. Ця процедура буде застосовуватись на постійній основі у зв'язку з вимогою до постійної ротації ключів. Пропонується застосувати для генерації цих ключів **ДСТУ 9041:2020**. Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса [11], що містить також алгоритм генерування псевдовипадкових послідовностей. Іншим варіантом є застосування фізичного генератора для генерування випадкових послідовностей (наприклад, шляхом зняття показників паразитних ємностей транзисторів тощо) [12].

Система впізнавання включає (рисунок 1):

- головний центр впізнавання;
- центри впізнавання (зазвичай – встановлені на комплексах РЛС);
- центри запуску повітряних об'єктів (аеропорти та підрозділи, що мають на озброєнні БпАК);
- повітряні об'єкти (пілотовані та безпілотні);
- наземні об'єкти*;
- водні та підводні об'єкти*.

* В даній роботі розглядаються переважно повітряні об'єкти. У випадку розширення роботи системи впізнавання «свій-чужий» на наземні та водні об'єкти, до складу системи впізнавання слід включити штаби (для розподілу ключів від головного центру впізнавання наземним об'єктам) та порти (для водних/підводних об'єктів). При цьому, оскільки кораблі та підводні човни можуть виконувати завдання автономно впродовж більше ніж одного дня, цю специфіку також слід окремо враховувати при реалізації ліній впізнавання «літак-корабель», «корабель-літак» і т.д.

Загальна схема роботи системи впізнавання «свій-чужий» (рисунок 2):

1. Головний центр впізнавання генерує випадкові ключі (загальні та індивідуальні, для впізнавання за принципом «Хто ти?») для застосування в системі. На кожен день генеруються нові ключі. В цьому випадку навіть у випадку компрометації поточних ключів вже наступного дня система знову буде захищеною.
2. В кінці кожного дня ключі, згенеровані головним центром впізнавання, централізовано розсилаються центрам розпізнавання та центрам запуску повітряних об'єктів (за потреби – штабам та ін.).
3. Ключі на сьогодні перед кожним вильотом пілотованих та безпілотних літальних апаратів зберігаються в їх пам'яті.

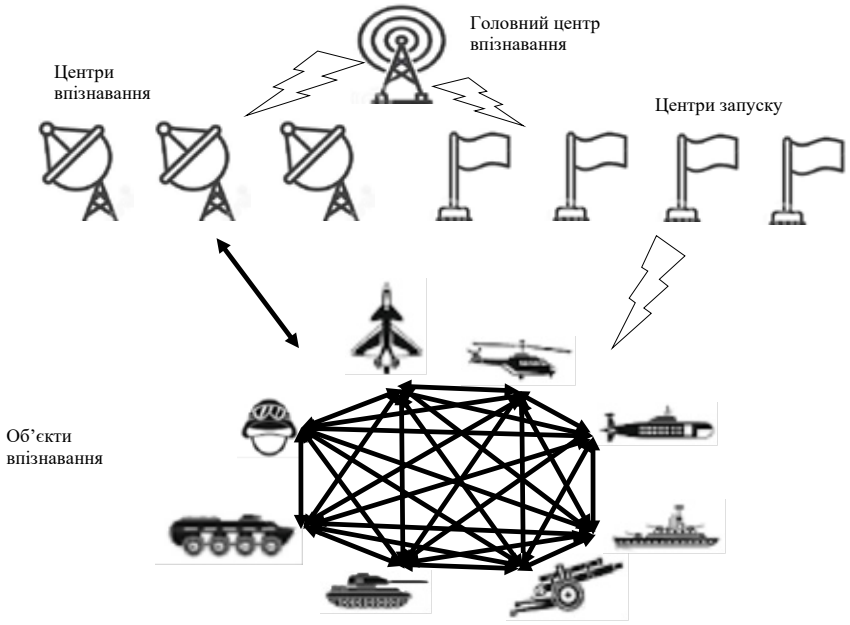

Рис. 1. Склад системи впізнавання «свій-чужий»

Рис. 2. Загальна схема роботи системи впізнавання «свій-чужий»

4. Під час виконання завдання за необхідності відбувається впізнавання за потрібною лінією впізнавання.

Розробка алгоритму ідентифікації об'єктів типу «свій-чужий». У зв'язку з наявністю двох суперечливих вимог до системи державного впізнавання (впізнавання має відбутись якнайшвидше, щоб запобігти дружньому вогню – але воно має бути надійним, щоб ворог не зміг обманути та оминути систему ППО), **впізнавання пропонується виконувати в два етапи**:

1. Етап 1. Максимально швидке, але не гарантовано надійне впізнавання. Не відповідає на питання «Хто ти?», «Де ти?».
2. Етап 2. Більш повільний, але й краще захищений етап, що пересвідчується в правильності впізнавання об'єкту. Може відповідати на питання «Хто ти?», «Де ти?».

Ці етапи визначають статуси об'єктів в системі державного впізнавання (рисунок 3):

Рис. 3. Статуси об'єктів в системі державного впізнавання

1. **«Невідомий»**. До першого етапу впізнавання об'єкт, до якого застосовується процедура впізнавання, вважається «невідомим».
2. **«Ймовірно свій»**. Цей статус призначається об'єкту, що успішно пройшов перший етап впізнавання.
3. **«Свій»**. Цей статус призначається об'єкту, що успішно пройшов другий етап впізнавання.
4. **«Чужий»**. Цей статус призначається об'єкту, що провалив перший або другий етап впізнавання.

Якщо системи ППО будуть інтегровані з системою державного впізнавання, то статус означатиме можливість застосування засобів ППО проти повітряної цілі:

1. **«Невідомий»** – надсилається запит на впізнавання. По відсутності коректної відповіді до таймауту – засоби ППО застосовуються в автоматичному режимі.
2. **«Ймовірно свій»** – засоби ППО не застосовуються в автоматичному режимі – але можуть застосовуватись у ручному режимі (на випадок компрометації першого етапу впізнавання ворогом та визначення цілі як ворожої за поведінкою або шляхом візуального впізнавання).
3. **«Свій»** – засоби ППО блокуються від застосування по своїх цілях.
4. **«Чужий»** – засоби ППО застосовуються в автоматичному режимі.

Розглянемо розроблений швидкий, але не гарантовано надійний **алгоритм Етапу 1**:

1. Як було описано вище в загальній схемі роботи системи впізнавання Головний центр впізнавання генерує випадкові ключі (загальні для усіх об'єктів системи впізнавання) терміном дії 24 години. Для етапу 1 генеруються три ключі – ключ запиту $KI1$ довжиною 128 бітів, а також ключ відповіді $KI2$ довжиною 64 біти. Ці два ключі будуть загальними для усіх центрів та об'єктів впізнавання. Крім того, генерується достатня кількість випадкових ідентифікаторів запиту одноразового використання IZ_i, i= 1…N, кількість яких N залежить від очікуваних обсягів процедур запиту-відповіді державного впізнавання впродовж наступних 24 годин, кожен довжиною 128 бітів. Кожного дня головний центр генеруватиме нові набори з N IZ_i, $KI1$ та $KI2$, при цьому краще згенерувати більшу кількість ідентифікаторів запиту N, ніж недостатню – щоб був запас на випадок неочікуваного зростання активності в контрольованому повітряному просторі.
2. Ключі та ідентифікатори запиту розподіляються між центрами впізнавання та центрами запуску (аеропорти, підрозділи, що мають на озброєнні БпАК тощо). При цьому усім надаються ключі $KI1$ та $KI2$, але кожен отримує власну диз'юнктну підмножину P_j (j=1…M, де M – кількість центрів впізнавання та запуску) з усієї множини N IZ_i – тобто кожна підмножина:

$$P_j \subset N$$

При цьому:

$$P_1 \cap P_2 = P_1 \cap P_3 = \ldots = P_{M-1} \cap P_M = \varnothing$$

Тобто жодна підмножина не має загальних з будь-якою іншою підмножиною елементів.

3. Перед вильотом на завдання з центру запуску об'єкту впізнавання (літаку, БПЛА тощо) передають ключі $KI1$ та $KI2$, а також диз'юнктну підмножину P_{jk} (k=1…S, де S – це очікуваний, запланований обсяг запитів від об'єкту впізнавання) підмножини P_j IZ_i.
4. Для проведення Етапу 1 процедури впізнавання запитувач (за будь-якою з ліній впізнавання алгоритм незмінний) формує запит: операцією виключної диз'юнкції (що також має назви виключне АБО, XOR та гамування) шифрує ключем $KI1$ ще не використаний до цього ідентифікатор запиту одноразового використання IZ_i, на виході отримуємо зашифрований запит на впізнавання R_a обсягом 128 біт, який відсилається відповідачу:

$$R_a = KI1 \oplus IZ_i$$

5. Відповідач (наприклад, БПЛА), отримує запит R_a.

6. Відповідач використовує ключ $KI1$ і операцією виключної диз'юнкції розшифровує отриманий запит R_a (завдяки подвійній операції XOR з використанням ключа $KI1$ він видаляє сам себе):

$$R_b = KI1 \oplus R_a = KI1 \oplus KI1 \oplus IZ_i = \mathrm{IZ_i}$$

7. Відповідач виконує операцію виключної диз'юнкції над першою та другою половинами розшифрованого ідентифікатора $\mathrm{IZ_i}$ – IZ_i1 та IZ_i2 – між собою:

$$R_b = IZi1 \oplus IZ_i2$$

Таким чином відповідач отримує блок R_b довжиною 64 біти.

8. Відповідач шифрує отриманий блок R_b операцією виключної диз'юнкції з ключем $KI2$:

$$R_c = R_b \oplus KI2$$

9. Відповідач відсилає запитувачу відповідь R_c.

10. Запитувач розшифровує отриману відповідь R_c ключем $KI2$:

$$R_d = R_c \oplus KI2 = R_b \oplus KI2 \oplus KI2 = R_b$$

11. Запитувач одразу після кроку 4 виконує ту ж дію, що і відповідач на кроку 7 – операцію виключної диз'юнкції над першою та другою половинами використаного ідентифікатора IZ_i для отримання контрольного значення:

$$R_k = IZi1 \oplus IZ_i2$$

12. Після отримання та розшифрування відповіді від відповідача запитувач порівнює розшифровану відповідь R_d з контрольним значенням R_k. Якщо вони співпадають – відповідач успішно пройшов перевірку та отримує статус «Ймовірно свій».

Можливе також додаткове спрощення та пришвидшення Етапу 1 – якщо відмовитись від використання ключа $KI2$, та викинути кроки 8 та 10, то ціною незначного зменшення надійності системи можна позбутись двох операцій шифрування/дешифрування.

Аналіз підходів до криптоаналізу Етапу 1 розробленого алгоритму. Розглянемо, які дані зловмисник зможе отримати з перехопленого в радіоефірі обміну запитом та відповіддю.

Зловмисник має змогу перехопити два повідомлення, що передавались радіоефіром – запит $R_a = KI1 \oplus IZ_i$ на кроці 4 та відповідь $R_c = R_b \oplus KI2$ на кроці 9.

Якщо представити відкритий ключ $KI1$ та ідентифікатор IZ_i у вигляді двох частин по 64 біти кожна (відповідно KI_{11} та KI_{12}, а також $IZi1$ та IZ_i2), то супротивник в запиті може перехопити:

$$\mathrm{DATAPACK1} = \begin{cases} KI_{11} \oplus IZ_i1 \\ KI_{12} \oplus IZ_i2 \end{cases}$$

У відповіді він може перехопити:

$$\mathrm{DATAPACK2} = IZ1_i \oplus IZ2_i \oplus K_{I2}$$

Оскільки усі початкові дані, що повинні лишатись прихованими від супротивника (KI_{11}, KI_{12}, $KI2$, а також $IZ1_i$ та $IZ2_i$), за статистичними характеристиками мають не відрізнятись від випадкових, то засоби статистичного аналізу не зможуть дати супротивнику жодних підказок щодо цих початкових даних за перехопленими даними.

Якщо він спробує скористатись перехопленими даними, щоб дізнатись щось більше, виконуючи операцію гамування, то він зможе отримати такі варіанти:

$$KI_{11} \oplus IZ2_i \oplus KI2$$

$$KI_{12} \oplus IZ_{21} \oplus KI2$$

$$KI_{11} \oplus IZ2_i \oplus KI_{12} \oplus IZ2_1$$

$$KI_{11} \oplus KI_{12} \oplus KI2$$

Якщо зловмисник надійшле (з метою визначення секретних ключів) фальшивий запит на впізнавання відповідно до Етапу 1, наприклад (для спрощення розуміння), він складатиметься з усіх нулів – то відповідач виконає на цьому запиті операцію розшифрування, отримавши послідовність з двох половин ключа KI1 – KI_{11} та KI_{12}, далі виконає операцію гамування над цими ключами – KI_{11} та KI_{12} – а далі виконає операцію гамування отриманого результату з ключем $KI2$ – і надійшле отриманий результат зловмиснику.

Тобто, зловмисник знову ж таки отримає послідовність $KI_{11} \oplus KI_{12} \oplus KI2$ (або, у випадку використання спрощеного алгоритму Етапу 1 – $KI_{11} \oplus KI_{12}$).

Оскільки статистичні характеристики ключів та ідентифікаторів не відрізнятимуться від випадкових, отримані дані не дадуть зловмиснику жодної корисної інформації про значення KI_{11}, KI_{12} та $KI2$ – існує дуже велика (обмежена лише розмірністю ключів) кількість варіантів наборів KI_{11}, KI_{12} та $KI2$ (або в спрощеному випадку – KI_{11} та KI_{12}), що відповідатимуть відомим зловмиснику даним. І в нього не буде можливості визначити, який саме

варіант з цієї множини є вірним, без того, щоб послідовно їх перебирати, використовуючи в якості відповіді на запит до об'єкту впізнавання, стикаючись з усіма наслідками того, що після невірної відповіді цей об'єкт буде позначений системою впізнавання статусом «чужий».

Тепер після цього аналізу опишемо **переваги Етапу 1 впізнавання**:

1. **Етап 1 є максимально швидким та не вимагає багато ресурсів**. Для підготовки запиту запитувачу слід виконати лише одну операцію виключної диз'юнкції (XOR або гамування) двох блоків даних по 128 біт кожен. Довжина запиту також складає усього 128 біт. Відповідач має виконати три операції виключної диз'юнкції, першу – для блоків даних по 128 біт кожен, другу і третю – для блоків по 64 біти кожен. Відповідь на запит має довжину усього 64 біти. В пам'яті відповідача (якщо не планується, що він буде виконувати процедуру впізнавання в якості запитувача) мають зберігатись лише два ключі загальним обсягом 192 біти та бути наявним стільки ж вільної пам'яті.
2. **Етап 1 впізнавання є достатньо надійним**. Жодні дані при ньому не передаються у відкритому вигляді. Для шифрування використовується операція виключної диз'юнкції, що є вразливою до атаки по відомому відкритому тексту. Але у випадку, коли кожен ідентифікатор запиту використовуються виключно один раз, а усі ідентифікатори запиту та ключі шифрування згенеровані дійсно випадковим чином, то гамування забезпечує достатню стійкість, бо:

a) текст та пароль мають однакову довжину;

b) жодні дані в повідомленні (ідентифікатори запитів) не використовуються більш ніж один раз (обернена вимога до «жоден пароль не використовується більш ніж один раз);

c) як пароль, так і повідомлення є випадковими та не можуть бути вгадані як за словником, так і іншими методами (підсилена вимога у порівнянні з класичною «пароль є випадковим»);

d) якщо розглядати ідентифікатори запитів як одноразові ключі, то у випадку відсутності жодних статистичних закономірностей при їх генерації алгоритм наближається до абсолютно стійкого.

3. У зв'язку з фізичними особливостями та обмеженнями процедури впізнавання (блокування повторних запитів на деякий час задля запобігання обробці відбитих сигналів за бічними пелюстками від радіолокатора багатоканальних приймачів) вона є захищеною від атак перебором (bruteforce). Додатково можна встановити таймаути та блокування відповіді на запити від того ж запитувача після певної кількості спроб.

Недоліки Етапу 1 впізнавання:

1. Не дає відповіді на питання «Хто ти?» та «Де ти?».
2. Будь-хто може видати себе за легітимний запитувач. При виконанні Етапу 1 впізнавання відповідач не може перевірити легітимність запиту – і тому відповідатиме на будь-який запит такого формату, в тому числі від супротивника, що надсилає випадкові 128 біт запиту, не знаючи жодного з ключів та ідентифікатора. Це не дасть супротивнику будь-якої корисної інформації – але може видати місцезнаходження відповідача.
3. Не забезпечує захисту від атак типу "man in the middle". Якщо ворожий об'єкт впізнавання отримає запит Етапу 1 та надійшле його легітимному об'єкту впізнавання, а потім передасть його відповідь до запитувача, то він зможе видати себе за легітимний об'єкт впізнавання. Ймовірність цього можна зменшити обмеженням максимального часу очікування відповіді, але теоретична можливість проведення такої атаки залишається.
4. Вимагає щоденної генерації великої кількості ідентифікаторів впізнавання.

Для компенсації цих недоліків далі слід застосувати алгоритм Етапу 2.

Слід зважити, що у випадку повторного використання ідентифікатора запиту, який вже був використаний раніше та разом з відповіддю на нього став відомий супротивнику, його повітряний об'єкт може надіслати таку ж відповідь на цей запит, і центр впізнавання розпізнає цю відповідь, як вірну. Тому ідентифікатори запитів мають використовуватись один і лише один раз, ця вимога є обов'язковою для забезпечення достатнього рівня надійності першого етапу впізнавання.

Альтернативою застосуванню централізованій генерації та розподілу випадкових ідентифікаторів запитів є генерація цих ідентифікаторів генераторами випадкових чисел, встановленими на апаратурі центрів впізнавання та об'єктів впізнавання. Але такий підхід має три **недоліки**:

1) Оскільки ідентифікатори будуть генеруватись незалежно, вони можуть повторюватись. У випадку згенерованого дублікату ідентифікатора запиту, зашифрований запит впізнавання буде ідентичним до того, що вже використовувався сьогодні. Тож, якщо супротивник зберіг той запит та відповідь на нього, то він зможе продублювати цю відповідь, що призведе до успішного проходження ним Етапу 1 впізнавання. Хоча така ситуація (перехоплення попередньо переданих та наявність на ворожому об'єкті впізнавання саме тієї пари запиту та відповіді, що надсилались раніше) є малоймовірною, однак не неможливою. Тож такий підхід призведе до певного зменшення надійності Етапу 1.

2) Кожен об'єкт впізнавання повинен містити апаратуру для генерування випадкових ідентифікаторів запиту. І якщо для наземних об'єктів це не є принциповим – то, наприклад, для БпАК встановлення додаткової апаратури часто є проблематичним.

3) У випадку застосування спрощеного алгоритму Етапу 1 (без використання ключа $KI2$) вимоги до статистичних характеристик ідентифікаторів запиту значно зростуть, оскільки достатньо буде навіть невеликого відхилення цих характеристик від випадкових щоб створити ризик успішного криптоаналізу, визначення супротивником ключа $KI1$ та як наслідок – повної компрометації Етапу 1.

Етап 1 є однаковим для усіх ліній впізнавання «земля-літак», «літак-танк» і т.д. та використовує однакові ключі.

Можливе також використання відмінного (від того, що буде застосований на Етапі 2) частотного діапазону та значень потужності – для гарантованого завершення Етапу 1 навіть у випадку задіяних засобів РЕБ.

Тепер розглянемо **алгоритми Етапу 2 впізнавання.**

Суть роботи алгоритмів Етапу 2 – це обробка запитів і відповідей ОВТ, які зашифровані симетричним криптографічним алгоритмом. Такий підхід обрано тому, що, як і на Етапі 1, 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 РЕБ супротивника. Іншим підходом, що може використовуватись на етапі 2, є використання асиметричного криптографічного алгоритму лише для шифрування ключа симетричного алгоритму для його відправлення під час передачі сигналів запиту/відповіді. В цьому випадку можливість розшифрувати та використати ключ симетричного алгоритму автоматично означає наявність ключа асиметричного алгоритму.

Як зазначалось вище у вимогах до військових систем впізнавання, у відповідь ОВТ може надати не тільки свій ідентифікатор (якщо був надісланий запит «Хто ти?»), але й дані про координати, тип літака та ін., що може бути додатково використано для запобіганню підміні сигналу відповіді та перевірці справжності отриманого коду. ОВТ, включений у підсистеми Єдиної автоматизованої системи управління (ЄАСУ) ЗСУ, може також використовувати інформацію від цивільних систем для верифікації даних, отриманих через спеціальні мережі, що застосовують симетричні і асиметричні криптографічні алгоритми захисту інформації для забезпечення багаторівневого впізнавання ОВТ.

Розглянемо першим з варіантів розпізнавання на Етапі 2 найпростіший випадок – **алгоритм ідентифікації об'єктів типу «свій-чужий» для лінії впізнавання «земля-літак»**:

1) Як і на Етапі 1, напередодні у головному центрі впізнавання заздалегідь генерується відкритий довготерміновий ключ K_b для асиметричного алгоритму шифрування та передається (разом з ключами та ідентифікатором Етапу 1) безпечними каналами на кожний об'єкт впізнавання та центр впізнавання. Він зберігається і на кожному об'єкті впізнавання, і у центрах впізнавання для подальшого тривалого використання впродовж наступної доби (хоча для Етапу 2 допустимим є довше застосування). Пара до цього відкритого ключа – закритий ключ K_z – зберігається виключно у центрах впізнавання.

2) Кожному з W об'єктів впізнавання призначається свій унікальний ідентифікатор I_p, (p=1…W), що зберігається в його довготерміновій пам'яті. Довжина кожного ідентифікатора складає 128 біт, генеруються вони генератором випадкових послідовностей (як і ідентифікатори запитів Етапу 1). База усіх ідентифікаторів I_p також зберігається у кожному з центрів впізнавання.

3) Для кожного з W об'єктів впізнавання також генерується унікальний закритий ключ-ідентифікатор Qz_p. Усі вони зберігається у кожному з центрів впізнавання, а також свій закритий ідентифікатор зберігається в пам'яті відповідного об'єкта впізнавання (тобто він зберігає для Етапу 2 закритий ключ-ідентифікатор Qz_p, відкритий ідентифікатор I_p. – їх, за необхідності, можна передавати іншим об'єктам впізнавання – та ключ K_b).

4) За необхідності виконання процедури впізнавання центр впізнавання (запитувач) надсилає об'єкту впізнавання (відповідачу) зашифрований секретним ключем K_z запит на впізнавання B_r, що містить тип запиту (зарезервоване значення I_0 для «Хто ти?», у випадку «Де ти?» – запит також включає відкритий ідентифікатор об'єкту впізнавання, чиє місцезнаходження намагається визначити центр впізнавання), згенерований запитувачем псевдовипадковий сеансовий ключ $K1_{se}$ довжиною 256 біт, а також позначку дати та часу (включаючи секунди) T_{curr}. В якості криптографічного алгоритму в запиту використовується державний стандарт України для шифрування коротких повідомлень [сч14]. Тобто запит «Хто ти?» матиме вигляд:

$$\{I_0,\ K1_{se},\ T_{curr,}\}K_z$$

запит «Де ти?» матиме вигляд:

$$\{I_p,\ K1_{se},\ T_{curr,}\}K_z$$

5) Відповідач, отримавши запит на впізнавання B_r, розшифровує його відкритим довготерміновим ключем K_b. Якщо в результаті розшифровки отримані дані мають сенс, то це доводить, що надсилач запиту (центр впізнавання) знає секретний ключ K_z – а отже є легітимним запитувачем.

6) Перевіряється також відхилення відмітки часу в запиті T_{curr} від часу на системному годиннику відповідача. Якщо відмінність є більшою за встановлене обмеження похибки – це означає, що або запит є повтором запита, що використовувався раніше, і надсилає його зловмисник, або в запитувача збитий системний годинник. В будь-якому з цих випадків запит відкидається та ігнорується.

7) Якщо розшифрований запит містить будь-який ідентифікатор, крім ідентифікатора відповідача чи зарезервованого значення I_0 (тобто отриманий запит є запитом «Де ти?», що адресований іншому відповідачеві), то цей запит також відкидається та ігнорується.

8) Якщо ж розшифрований запит містить або ідентифікатор саме цього запитувача (тобто це запит «Де ти?», адресований саме йому), або ідентифікатор I_0 (тобто це запит «Хто ти?») – відповідач готує відповідь на запит.

9) В будь-якому з описаних в пункті 7 випадків, коли відповідач *p* мусить надіслати відповідь, то ця відповідь від об'єкта впізнавання *p* складається з двох частин. Перша призначена для того, щоб запитувач дізнався, хто саме є відповідачем. Вона містить відкритий ідентифікатор відповідача I_p. Перша частина відповіді шифрується сеансовим ключем $K1_{se}$, що був надісланий у зашифрованому вигляді. Друга містить отриману відмітку часу T_{curr}, змінену на 1 та згенерований відповідачем псевдовипадковий сеансовий ключ $K2_{se}$ довжиною 256 біт. Другу частину відповіді зашифровано закритим ключем-ідентифікатором Qz_p. Для шифрування в обох випадках використовується державний стандарт симетричного шифрування ДСТУ 7624:2014 [сч17]. Знання сеансового ключа $K1_{se}$ відповідачем підтверджує, що йому відомий відкритий довготерміновий ключ K_b і то є відповідь саме на надісланий нині запит, а не копія відповіді іншого об'єкта впізнавання. Тобто відповідь етапу 2 має вигляд:

$$\{I_p\}K1_{se} + \{ T_{curr+1} ,K2_{se}\}Qz_p$$

10) Центр впізнавання спочатку розшифровує першу частину відповіді сеансовим ключем $K1_{se}$ і тепер він точно знає, хто є відповідачем (і має довготерміновий відкритий ключ K_b). Далі він знаходить в таблиці секретний ключ-ідентифікатор Qz_p, що відповідає відкритому ідентифікатору I_p. Після цього запитувач розшифровує ключем-ідентифікатором Qz_p другу частину відповіді і звіряє відмітку часу. Співпадіння підтверджує, що вона зашифрована саме ключем Qz_p, а відповідач – той, за кого він себе видає. Тобто в результаті отримання відповіді від об'єкту впізнавання (або від усіх об'єктів, що відповіли на загальний запит «Хто ти?») та розшифровки цієї відповіді, центр впізнавання знає, що відповідачу відомі секретний ключ-ідентифікатор Qz_p та відкритий довготерміновий ключ K_b.

11) Після етапу 10 і запитувач, і відповідач мають сеансовий ключ $K2_{se}$, що не передавався в ефірі у відкритому вигляді або зашифрованим тільки з використанням загальновідомого ключа K_b, тому без знання, який закритий ключ-ідентифікатор відповідає якому відкритому ідентифікатору об'єкта впізнавання, ворог не зможе отримати цей сеансовий ключ $K2_{se}$. Тому його можна вільно використовувати в якості ключа шифрування (з використанням ДСТУ 7624:2014) для захищеного обміну іншими необхідними даними.

12) У випадку, якщо один з об'єктів впізнавання втрачено, і він потрапив до рук ворога, слід передати інформацію про це усім центрам впізнавання. Оскільки на об'єкті впізнавання зберігався лише його власний секретний ідентифікатор, то хоча ворог дізнався довготерміновий ключ і зможе розшифровувати запити (до моменту ротації довготермінового ключа), але йому невідомі інші секретні ідентифікатори. І оскільки стандарт ДСТУ 7624:2014 забезпечує захист від атак по відомому вмісту повідомлення (в нашому випадку – це час T_{curr}), то навіть дізнавшись сеансовий ключ $K1_{se}$ запита, що призначений іншому об'єкту впізнавання, він не зможе без знання Qz_p (якого він не має) отримати доступ до сеансового ключа $K2_{se}$. А отже – не зможе й видати себе за інший об'єкт впізнавання.

У випадку, якщо інформація про захоплені супротивником/втрачені/знищені об'єкти впізнавання буде вчасно оновлюватись в базі даних центру керування повітряним рухом, то такий алгоритм забезпечуватиме достатню стійкість та надійність впізнавання [сч17]-[сч18]. Інакше ворог, захопивши об'єкт впізнавання, може просто перемістити 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.

Для інших ліній впізнавання (наприклад «літак-літак» чи «літак-танк») в якості модифікації описаного вище алгоритму Етапу 2 слід використовувати центр керування повітряним рухом або інший доступний для зв'язку обома вузлами лінії впізнавання центр впізнавання – в якості центру розподілу ключів, як це запропоноване в протоколі Kerberos [сч19].

Слід також зазначити, що для літальних апаратів, що діють в основному на ворожій території (були запущені біля лінії фронту, не намагаються рухатись вглиб контрольованої території і т.д.) може бути достатнім застосування лише Етапу 1 та статусу Ймовірно свій. Це актуально для малих БПЛА, на яких складно знайти місце та ресурси для встановлення апаратури, здатної виконувати алгоритм Етапу 2.

Розроблений алгоритм має вищу швидкодію порівняно з тим, що використовується на сьогоднішній день (особливо якщо говорити про Етап 1) та забезпечує вищий рівень надійності завдяки використанню сучасних криптографічних алгоритмів, що відповідають державним стандартам України.

Висновки

На основі визначених переваг та недоліків поточного алгоритму державного впізнавання запропоновано новий двоетапний алгоритм захисту інформації типу «запит-відповідь» для системи державного впізнавання для військових об'єктів, побудований на основі державних стандартів України, що забезпечуватиме достатню масштабованість, стійкість, надійність та багаторівневість впізнавання. Виконано аналіз розробленого алгоритму, його переваг та недоліків порівняно з алгоритмом, що застосовується на даний момент. Визначені можливі підходи до криптоаналізу запропонованого алгоритму та проаналізовано їх застосовність та ефективність.

Алгоритм може застосовуватись не тільки для ліній впізнавання «земля-літак», але й для таких, як «літак-літак», «літак-танк», «літак-корабель» та ін. (в тому числі, в зворотному напрямі), включаючи навіть «літак-піхотинець».

Розроблений алгоритм має вищу швидкодію порівняно з тим, що використовується на сьогоднішній день (особливо якщо говорити про Етап 1) та забезпечує вищий рівень надійності завдяки використанню сучасних криптографічних алгоритмів, що відповідають державним стандартам України.

Список використаної літератури

1. Rudinskas D., Goraj Z., Stankūnas J. Security Analysis Of UAV Radio Communication System. Aviation. 2009. 13 (4). P. 116-121. doi: 10.3846/1648-7788.2009.13.116-121
2. Огурцов М.І. Розробка протоколу захищеного обміну даними для спеціальних мереж / Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, Кам'янець-Подільський національний університет імені Івана Огієнка; [ред-кол.: О.М.Хіміч (відп. ред.) та ін.]. – Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2019. – Вип. 19. – С. 108–113.
3. Matt, Brian J. Lightweight and Survivable Key Management for Army Battlefield Networks. Internal Publication, Network Associates Laboratories (2003).
4. Закревский О. Свой – чужой, 11 червня 2014. – Режим доступу: https://dou.ua/forums/topic/10097/
5. STANAG 4193. Technical Characteristics Of The IFF Mk XIIA System. NATO, 2016. p. 45.
6. Камалтинов, Г. Г. та ін. Впізнавання об'єктів на полі бою. Аналіз світового досвіду. Озброєння та військова техніка, 4, 2016. – с. 22-26. doi: 10.34169/2414-0651.2016.4(12).22-26
7. Putatunda, Rohan, et al. Camouflaged object detection system at the edge. Automatic Target Recognition XXXII. Vol. 12096. SPIE, 2022. doi: 10.1117/12.2618869
8. Pearce, Nolan, and Stephen Hamilton. «IFF using Beamforming in Telemetry Beacons.» 2021 IEEE Western New York Image and Signal Processing Workshop (WNYISPW). IEEE, 2021. doi: 10.1109/wnyispw53194.2021.9661287
9. Ермак, С.Н. Касанин, О.А. Хожевец С.Н. Устройство и эксплуатация наземных средств системы государственного опознавания. Минск: БГУИР, 2017. 230 с.
10. Канащенков А.И., Меркулов В.И. Радиолокационные системы многофункциональных самолетов. М.: Радиотехника, 2006. 656 с.
11. ДСТУ 9041:2020. Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. – Режим доступу: https://cip.gov.ua/ua/news/2020-roku-zaprovadzheno-novii-nacionalnii-standart-dstu-9041-2020
12. Жуйков В.Я., Терещенко Т.О., Ямненко Ю.С., Мороз А.В. Регульовані фільтри джерел живлення для захисту інформації в мікроконтролерах. Монографія. – Київ, 2016 – 184 с.

References

1. Rudinskas D., Goraj Z., Stankūnas J. Security Analysis Of UAV Radio Communication System. Aviation. 2009. 13 (4). P. 116-121. doi: 10.3846/1648-7788.2009.13.116-121
2. Ogurtsov M. I. Rozrobka protokolu zakhyshchenoho obminu danymy dlya spetsial′nykh merezh [Development of a secure data exchange protocol for special networks]. Matematychne ta komp'yuterne modelyuvannya. Seriya: Tekhnichni nauky: zb. nauk. prats′. Kam'yanets′-Podil′s′kyy natsional′nyy universytet im. Ivana Ohiyenka, 2019. 19. P. 108-113. (in Ukrainian).
3. Matt, Brian J. Lightweight and Survivable Key Management for Army Battlefield Networks. Internal Publication, Network Associates Laboratories (2003).
4. Zakrevskui O. (2014) Svoy – chuzhoy [Friend-or-foe]. [Online] June 11, 2014. Available at: https://dou.ua/forums/topic/10097/ [Accessed: 2nd November 2022].
5. STANAG 4193. Technical Characteristics Of The IFF Mk XIIA System. NATO, 2016. p. 45.
6. Kamaltinov G.G., et al. (2016) Vpiznavannya ob'yektiv na poli boyu. Analiz svitovoho dosvidu [Recognition of objects on the battlefield. Analysis of world experience]. Armament and military equipment. 4. p. 22-26. doi: 10.34169/2414-0651.2016.4(12).22-26
7. Putatunda, Rohan, et al. Camouflaged object detection system at the edge. Automatic Target Recognition XXXII. Vol. 12096. SPIE, 2022. doi: 10.1117/12.2618869
8. Pearce, N. and Hamilton, S., 2021, October. IFF using Beamforming in Telemetry Beacons. In 2021 IEEE Western New York Image and Signal Processing Workshop (WNYISPW) (pp. 1-5). IEEE. doi: 10.1109/wnyispw53194.2021.9661287
9. Ermak, S.N., Kasanin, O.A., Khozhevets, S.N. Ustroystvo i ekspluatatsiya nazemnykh sredstv sistemy gosudarstvennogo opoznavaniya [The Construction and Operation Principles of Ground Means of the State Identification System]. Minsk: BGUIR, 2017.
10. Kanashchenkov A.I., Merkulov V.I. Radiolokatsionnyye sistemy mnogofunktsional'nykh samoletov [Radar systems of multifunctional aircraft]. M.: Radiotehnika. 2006. 656 p.
11. DSTU 9041:2020. Informatsiyni tekhnolohiyi. Kryptohrafichnyy zakhyst informatsiyi. Alhorytm shyfruvannya korotkykh povidomlen′, shcho gruntuyet′sya na skruchenykh eliptychnykh kryvykh Edvardsa [Information Technology. Cryptographic protection of information. Short Message Encryption Algorithm Based on Twisted Edwards Elliptic Curves]. – (in Ukrainian) Available from: https://cip.gov.ua/ua/news/2020-roku-zaprovadzheno-novii-nacionalnii-standart-dstu-9041-2020 [Accessed: 2nd November 2022].
12. Zhuykov V.Y. et al. Rehul′ovani fil′try dzherel zhyvlennya dlya zakhystu informatsiyi v mikrokontrolerakh [Adjustable power supply filters to protect information in microcontrollers]. Monograph. Kyiv, 2016. 184 p.