УДК 004.056.5

DOI: 10.18372/2073-4751.77.18652

Грушак С.С.,
orcid.org/0009-0005-8229-5053,
e-mail: sg.grusha@ukr.net,
Гузій М.М., к.т.н.,
orcid.org/0000-0003-4807-8862,
e-mail: nn05@ukr.net,
Безвершенко Є.І.,
orcid.org/0000-0002-8068-1576,
e-mail: bezvershenko@gmail.com

ГІБРИДНІ КРИПТОСИСТЕМИ ЗАХИСТУ ВУЗЛІВ МЕРЕЖ FANET: ПІДХОДИ ДО ВИКОРИСТАННЯ

Національний авіаційний університет

Вступ

Однорангові самоорганізовані мережі *Flying Ad-Hoc Network* (*FANET*) для групи безпілотних літальних апаратів (БПЛА) набули розповсюдження та широко використовуються у цивільній, комерційній та військовій сферах. Організація взаємодії вузлів сенсорної мережі БПЛА відбувається для виконання завдань спостереження, моніторингу, виявлення та розпізнавання об'єктів, безпеки транспортних засобів, керування системами реального часу.

Швидка зміна топології мережі, активний рух у 3*D* просторі, завади природнього та штучного походження призводять до ускладнення передачі даних на фізичному, канальному, мережевому та транспортному рівнях відповідно до вимог *QoS*.

Відкритий канал передачі даних між вузлами мережі *FANET* потребує захисту від несанкціонованого доступу. Передача даних між вузлами у мережах *FANET* потребує удосконалення алгоритмів та протоколів автентифікації сторін та шифрування каналу зв'язку.

Сучасні сенсорні мережі БПЛА використовують переважно симетричні криптосистеми, але особливості їх функціонування (динамічна топологія, обмеженість енергетичних та обчислювальних ресурсів) вимагають розробки нових перспективних підходів, зокрема використання гібридних криптосистем.

Аналіз публікацій за темою дослідження

У роботі [1] розглянуто розповсюджені типи атак на сенсорні мережі безпілотних систем та криптографічні методи захисту від атак. Особлива увага приділена поточному стану використовуваних криптосистем, приведено детальний опис конкретних криптографічних алгоритмів.

Інформація щодо основних характеристик мереж *FANET* приводиться у роботі [2], визначено їх вплив на функціонування мережі.

Новий протокол *LAPEC* для автентифікації БПЛА запропоновано у роботі [3]. Протокол описує використання методів криптографії на еліптичних кривих для забезпечення додаткового рівня захисту у наявні процеси обміну даними між вузлами мережі.

Стан проблеми та постановка завдання дослідження

Характерними особливостями, які суттєво впливають на процеси обміну даними між вузлами мережі *FANET* є мобільність, щільність, геолокація та енергоспоживання вузлів, динамічна мережева топологія.

1) Мобільність вузлів: вузли мереж *FANET* можуть переміщуватись зі швидкістю до 400 км/год. Збільшення швидкості БПЛА призводить до втрат зв'язку, помилок при передачі даних;

2) Топологія мережі: топологія мереж *FANET* постійно змінюється через

високу мобільність вузлів. У випадку зв'язку безпосередньо усіх вузлів зі станцією наземного управління (*GCS*) використовується топологія зірка, а у випадку часткової відсутності зв'язку виникає необхідність у динамічній маршрутизації з сітчастою (*Mash*) топологією (рис. 1);

3) Енергоспоживання: обмеження у енергетичних ресурсах – критична проблема усіх однорангових самоорганізованих мереж. У випадку мереж *FANET* енергоспоживання залежить від розмірів вузла, відстані зв'язку, апаратного та програмного забезпечення тощо. Зменшення енергоспоживання безпосередньо впливає на час функціонування мережі та стабільність зв'язку між її вузлами.

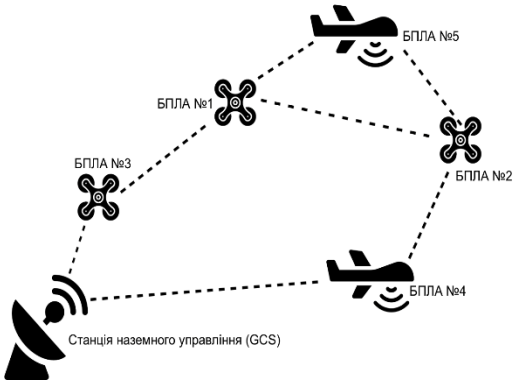

Рис. 1. Мережа *FANET* з динамічною *Mash*-топологією

Обмін даними між вузлами мережі *FANET* відбувається по відкритому бездротовому каналу зв'язку. Через незахищеність комунікаційного середовища ці процеси є вразливими до атак різного типу: посередника (*MITM*), підслуховування, повторення. Проблеми безпеки перешкоджають ефективному використання БПЛА, ускладнюють їх комунікаційні протоколи.

Симетричні криптосистеми набули широкого використання у технологіях шифрування даних між БПЛА [1]. Зазвичай для цієї мети використовуються блочні алгоритми шифрування, що надають можливість шифрувати та дешифрувати дані за допомогою єдиного секретного ключа. Сучасним прикладом таких алгоритмів є *AES* та *ChaCha*20. Недоліком використання симетричних криптосистем є необхідність обміну сторонами секретними ключами до сеансу зв'язку. Гібридні криптосистеми поєднують переваги швидкодії симетричних та захищеності асиметричних криптографічних систем, забезпечують захист генерації секретного ключа та дозволяють автентифікувати сторони зв'язку.

У випадку мереж *FANET* вищезазначені процедури ускладняються. На заваді їх виконання лежить динамічна природа мереж *FANET*. Непрогнозована зміна мережевої топології спричиняє корегування таблиць маршрутизації, що призводить до втрати пакетів даних та збільшення енергоспоживання для повторних спроб їх пересилання іншим маршрутом.

Метою дослідження є оцінка можливості використання гібридних криптосистем дла захисту ресурсів вузлів мережі *FANET*.

Основна частина. Технології гібридних криптосистем в сенсорних мережах FANET

Процеси передачі даних умовно поділяються на два етапи: обробки та передачі. Перший етап полягає у кодуванні, стисненні та шифруванні даних, а другий у безпосередній передачі даних адресату. Шифрування даних відбувається на рівні обробки, проте сучасні протоколи, що гарантують захист даних, завжди працюють ближче до рівня передачі. Наприклад, з точки зору моделі *OSI*, використання криптосистем для захищеної передачі даних відбувається на сеансовому рівні (рис. 2).

На початку сеансу зв'язку сторони узгоджують між собою конкретні протоколи та алгоритми шифрування, що будуть використовуватись ними у подальшому. Розглянемо сучасні протоколи та алгоритми шифрування даних.

1. *Transport Layer Sockets* (*TLS*). На сьогодні є де-факто стандартним протоколом, що описує процедури захищеної передачі даних через незахищені канали зв'язку, який працює над *TCP*/*UDP*. Протокол описує використання гібридної криптосистеми для шифрування каналу зв'язку, є перевіреним та надійним;

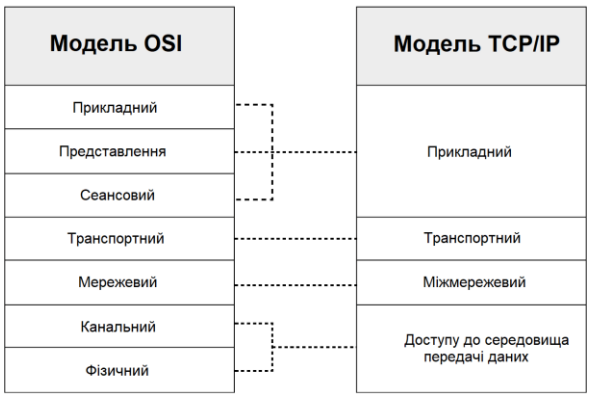

Рис. 2. Мережеві моделі *OSI* та *TCP/IP*

2. *Elliptic-curve Cryptography* (*ECC*). Асиметричний алгоритм шифрування даних у основі якого лежить використання криптографії з відкритим ключем;

3. *Advanced Encryption Standard* (*AES*). Симетричний алгоритм шифрування даних, що використовується у різних сферах.

Вищезазначені алгоритми використовуються в останній версії *TLS* 1.3, вони дозволяють вирішити задачі автентифікації сторін та шифрування даних.

Автентифікація сторін відбувається за допомогою сертифікатів формату *X*.509. Сертифікат містить сутність та пов'язаний з нею публічний ключ. Сутність та публічний ключ пов'язуються та затверджуються цифровим підписом центру сертифікації (*CA*).

На основі концепції протоколу *TLS* для вузлів мережі *FANET* розроблено наступний алгоритм автентифікації:

1. Створюється приватний ключ $PCA_{private}$ та пов'язаний з ним самопідписний сертифікат PCA_{cert}. Обидва виступатимуть у ролі приватного центру сертифікації (*PCA*);

2. PCA_{cert} додається до сховища довірених сертифікатів на кожному БПЛА;

3. Для вузла *A* створюється приватний ключ $A_{private}$ та пов'язаний з ним сертифікат A_{cert}, який у свою чергу підписується приватним ключем $PCA_{private}$;

4. Для вузла *B* створюється приватний ключ $B_{private}$ та пов'язаний з ним сертифікат B_{cert}, який у свою чергу підписується приватним ключем $PCA_{private}$;

5. Вузли *A* та *B* обмінюються сертифікатами A_{cert} та B_{cert}. Кожен вузол перевіряє цифровий підпис отриманого сертифіката за допомогою PCA_{cert}. Вузли взаємно пройшли процедуру автентифікації.

Для запропонованого алгоритму функція формування ключа виконується в пункті 5 після обміну сертифікатами. Вхідними параметрами функції є пари $A_{cert}B_{private}$ та $B_{cert}A_{private}$. Таким чином кожна сторона незалежно приходить до однакового секрету та у подальшому використовує його для симетричного шифрування (рис. 3).

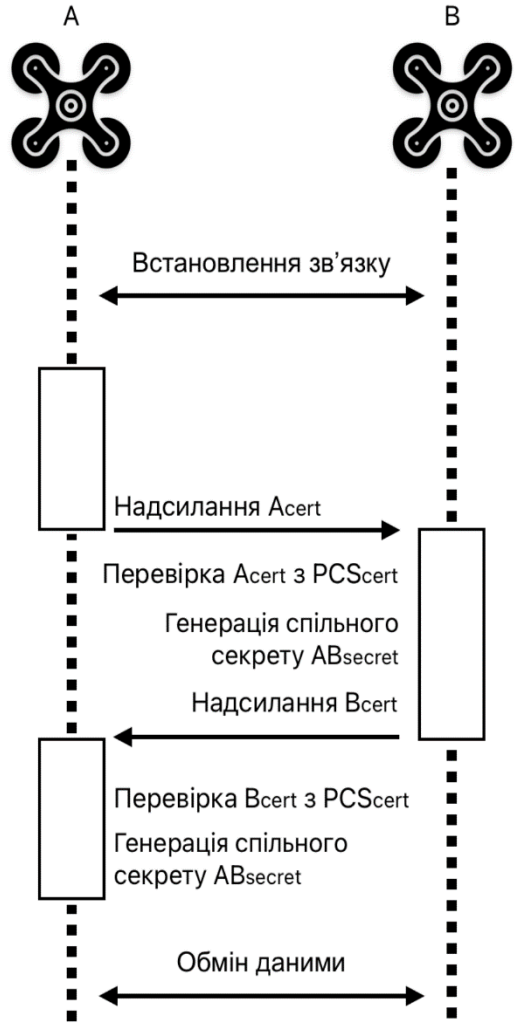

Рис. 3. Гібридна технологія шифрування даних між вузлами мереж *FANET*

До переваг запропонованого алгоритму відноситься можливість створювати самопідписні сертифікати. На відміну від глобальної мережі Інтернет, де існують складні ієрархії центрів сертифікації,

групи БПЛА можливо обслуговувати без третьої сторони. До недоліків можемо віднести загрозу компрометації приватного ключа та сертифікату БПЛА при втраті фізичного доступу до нього, проте існує механізм відклику цифрового підпису.

Недоліком методу є незмінність секретного ключа між сеансами зв'язку, проте для нового сеансу зв'язку кожна сторона може генерувати проміжні сертифікати.

Оскільки *FANET* є динамічною мережею, то маршрути між вузлами мережі часто та непередбачувано змінюються. Постає питання щодо підтримки актуальної таблиці маршрутизації, зберігання та відновлення сесій, ускладняється робота рівня передачі даних. Використання асиметричних алгоритмів шифрування може призвести до небажаних наслідків: при відновленні сесій необхідно повторно погодити алгоритми шифрування, виконати обмін сертифікатами, згенерувати секретні ключі. Складність обчислювальних алгоритмів призведе до збільшення енергоспоживання та зменшення автономності вузлів. З іншого боку, використання асиметричних алгоритмів та технік *TLS* 1.3 (*Pre-Shared Key, Session Resumption, Round Trip-Time Reduction*) дозволить вирішити задачі автентифікації вузлів, підвищить рівень безпеки за рахунок постійної зміни секретного ключа.

Розробка протоколів транспортного рівня для мереж *FANET* відбувається з врахуванням динамічних змін топології. На сьогодні існують приклади впроваджених протоколів з *IP* адресацією, тобто їх транспортний рівень підтримує *TCP*/*UDP* [4]. Додатково створені стандарти, в яких описуються процеси передачі даних між БПЛА (*Joint Architecture for Unmanned Systems*) та стандарт НАТО – *STANAG* 4586. У стандарті *JAUS* впроваджені обгортки навколо *TCP*/*UDP – JTCP*/*JUDP*, транспортні протоколи *FANET* підтримують *TCP*/*UDP*, що дозволяє використання безпосередньо *TLS*. При використанні інших транспортних протоколів можлива адаптація алгоритмів та технік з *TLS*.

Експериментальне дослідження впливу гібридних криптосистем на енергоресурси вузлів мереж FANET

Функціонування гібридної криптосистеми для шифрування даних потребує активного використання апаратних ресурсів *CPU* та *RAM*, що приводить до збільшення енергоспоживання.

Перед впровадженням додаткових обчислювальних процедур на вузлах мереж *FANET* критично важливо оцінити їх вплив на вищезазначені ресурси. Для порівняльного аналізу розглянемо енергоефективність виконання алгоритмів *AES* та *ECC*. З точки зору споживання ресурсів важливі наступні параметри: час виконання, кількість використаних циклів *CPU*, енергоспоживання.

Тестування проводилось на *Intel Core i*7-7700*HQ CPU* 2.80 ГГц. *TDP* – 45 Вт. Об'єм тестового набору даних 1024 байти. Алгоритми реалізовано з використанням криптографічної бібліотеки з відкритим вихідним кодом *OpenSSL*, яка отримала сертифікацію *FIPS* 140-2 федеральної програми США щодо тестування та сертифікації криптографічних модулів [5]. Програмний код розроблено з використанням *OpenSSL* 3 та розміщено на *GitHub* [6].

Результати моделювання роботи алгоритмів *AES* та *ECDSA* представлені у табл. 1 та наведені на рис. 4 - рис. 9.

Таблиця 1. Результати моделювання виконання алгоритмів *AES* та *ECDSA*

Алгоритм	Операція	Час виконання (мкс)	Кількість циклів *CPU*	Енергоспоживання (нВт)
*AES*_128_*GCM*	Шифрування	2.637	7391	25.1
	Дешифрування	2.491	6922	25.4
*AES*_192_*GCM*	Шифрування	2.642	7447	26
	Дешифрування	2.316	6570	25.2

Продовження таблиці 1.

AES_256_GCM	Шифрування	2.965	8363	30.8
	Дешифрування	2.604	7140	25.2
ECDSA (*secp*521*r*1)	Генерація приватного ключа та сертифіката	7.557	21222939	100
	Цифровий підпис	8.237	23080782	100,6
	Перевірка цифрового підпису	5.866	9065908	75
	Функція формування ключа	15.395	43227917	200

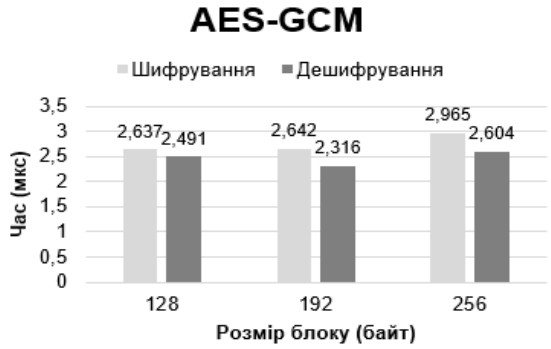

Рис. 4. Час виконання алгоритму *AES-GCM*

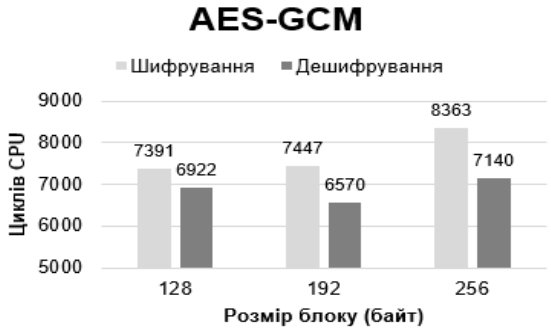

Рис. 5. Використані цикли *CPU* алгоритмом *AES-GCM*

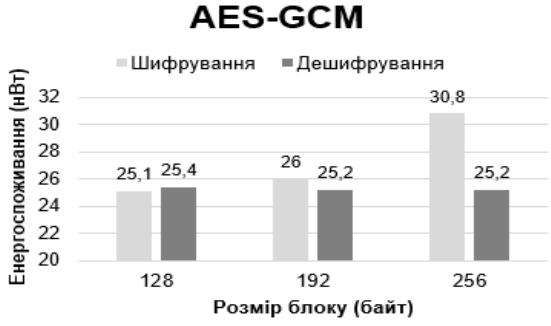

Рис. 6. Енергоспоживання алгоритму *AES-GCM*

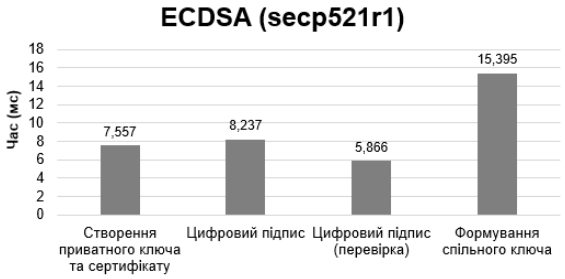

Рис. 7. Час виконання основних операцій алгоритмом *ECDSA*

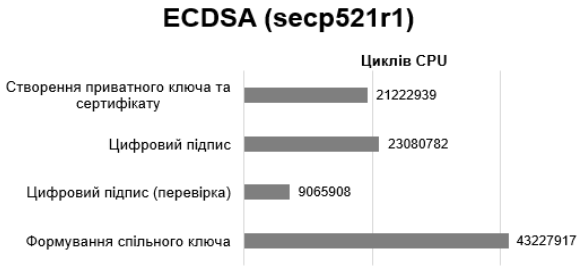

Рис. 8. Використані цикли *CPU* основними операціями алгоритму *ECDSA*

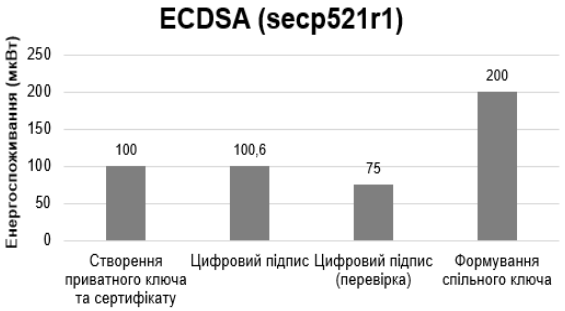

Рис. 9. Енергоспоживання основних операцій алгоритму *ECDSA*

Аналіз результатів проведених експериментальних досліджень дозволив виявити наступні закономірності.

1. Час виконання операцій симетричних та асиметричних алгоритмів

шифрування відрізняється на порядок 10^3. Операції асиметричних алгоритмів виконуються значно повільніше, а порядок часу їх виконання (мс) свідчить про необхідність потужної апаратної та програмної підтримки, виконання довготривалих ресурсоємних операцій. Проблему можливо вирішити за допомогою виконання розподілених обчислень на додаткових ядрах *CPU*;

2. Енергоспоживання *AES-GCM* є на порядок 10^3 менше, ніж *ECDSA*. З точки зору запропонованого алгоритму після встановлення зв'язку та взаємного обміну сертифікатами A_{cert} і B_{cert} кожна сторона виконуватиме операцію перевірки цифрового підпису та формування спільного ключа (рис. 3). Згідно результатів досліджень кожна сторона витратить на вищезазначені операції 275 мкВт енергії. Наприклад, у сучасного дрону *DJI Mavic* 2 ємність акумуляторних батарей становить 3850 мАч при напрузі у 15.4 В, тобто ресурс 59.29 Вт/год [7]. Орієнтовний час автономності дрона – до 1 години, а отже декілька десятків подібних операцій практично не впливатимуть на енергоспоживання;

3. Кількість використаних циклів *CPU* дозволяє оцінити мінімальні вимоги до параметру продуктивності *CPU*. Якщо розглядати операції зазначені у пункті 2, то для перевірки цифрового підпису та формування спільного ключа необхідно 52 293 825 циклів *CPU*. При тестуванні процесор з тактовою частотою 2.80 ГГц може виконати 53 такі операції на ядро, відповідно мінімальна тактова частота *CPU* має бути не менше 550 МГц;

4. Результати інших операцій *ECDSA* є сенс брати до уваги лише за умови, що вони будуть відбуватись безпосередньо на БПЛА. Як зазначено вище, операції створення приватного ключа, сертифікату та цифрового підпису можуть відбуватись на початку кожного сеансу зв'язку, або ж певними інтервалами. Сумарно по цим операціям використання електроенергії складає 200.6 мкВт, можлива кількість операцій на дроні *DJI Mavic* 2 – 295 314, а кількість циклів *CPU* не більша ніж у зазначених в пункті 3 операцій.

Висновки

Проведено аналіз сучасних технологій побудови захищених сенсорних мереж *FANET*.

Запропонована модель гібридної криптосистеми для шифрування даних, генерації спільного секретного ключа та автентифікації в мережі *FANET* на базі протоколу *TLS* та методів симетричного та асиметричного шифрування. Розроблено програмне забезпечення для тестування алгоритмів *AES-GCM, ECDSA* для операцій шифрування, дешифрування, створення секретного ключа, перевірки цифрового підпису. Для кожної операції проведені заміри часу виконання, визначена кількість циклів *CPU* та обсяги енергоспоживання.

В результаті проведених досліджень обгрунтована доцільність використання гібридних криптосистем вузлами мереж *FANET* за умови виконання певних вимог до апаратних, програмних та енергетичних ресурсів.

Література

1. Wiik J. H. Cybersecurity and cryptographic methods in unmanned systems. Kjeller : Norwegian Defence Research Establishment (FFI), 2020. P. 7–30.

2. Faezeh Pasandideh et al. A Review of Flying Ad Hoc Networks: Key Characteristics, Applications, and Wireless Technologies. *Remote Sensing*. 2022. Vol. 14, no.18. P. 1–10.

3. Shuo Zhang et al. A Lightweight Authentication Protocol for UAVs Based on ECC Scheme. *Drones*. 2023. Vol. 7, no. 5. 16 p.

4. İlker Bekmezci, Eren Şentürk, Tolgahan Türker. Security issues in flying ad-hoc networks (FANETs). *Journal of Aeronautics and Space Technologies*. 2016. Vol. 9, no. 2. P. 13–21.

5. Cryptographic Module Validation Program. URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4282.

6. Github: Graullon/openssl-test-suite. URL: https://github.com/Graullon/openssl-test-suite.

7. MAVIC 2 Specs. URL: https://www.dji.com/global/mavic-2/info.

Грушак С.С., Гузій М.М., Безвершенко Є.І.

ГІБРИДНІ КРИПТОСИСТЕМИ ЗАХИСТУ ВУЗЛІВ МЕРЕЖ FANET: ПІДХОДИ ДО ВИКОРИСТАННЯ

В статті представлені результати дослідження можливості використання гібридних криптосистем дла захисту вузлів сенсорної мережі FANET. Запропонована модель гібридної криптосистеми для шифрування даних, генерації спільного секретного ключа та розроблено алгоритм автентифікації в мережі FANET на базі протоколу TLS та методів симетричного/асиметричного шифрування. Виконано тестування алгоритмів AES-GCM, ECDSA для операцій шифрування, дешифрування, проведені заміри часових характеристик виконання операцій, визначена кількість циклів CPU та обсяги енергоспоживання.

В результаті проведених досліджень обгрунтована доцільність використання гібридних криптосистем вузлами мереж FANET за умови виконання певних вимог до апаратних, програмних та енергетичних ресурсів.

***Ключові слова**: мережа FANET; гібридна криптосистема; БПЛА; автентифікація; захист даних.*

Hrushak S.S., Huzii M.M., Bezvershenko E.I.

HYBRID CRYPTOSYSTEMS FOR THE PROTECTION OF FANET NETWORK NODES: APPROACHES TO USE

The article presents the results of research into the possibility of using hybrid cryptosystems to protect FANET sensor network nodes. A model of a hybrid cryptosystem for data encryption, generation of a shared secret key is proposed, and an authentication algorithm in the FANET network based on the TLS protocol and symmetric/asymmetric encryption methods is developed. AES-GCM, ECDSA algorithms were tested for encryption and decryption operations, time characteristics of operations were measured, the number of CPU cycles and energy consumption were determined.

As a result of the conducted research, the expediency of using hybrid cryptosystems by nodes of FANET networks is substantiated, provided that certain requirements for hardware, software and energy resources are met.

***Keywords**: FANET network; hybrid cryptosystem; UAV; authentication; data protection.*