DOI: https://doi.org/10.31392/NZ-udu-165.2026.23
УДК 355:[003.26:001.102-049.65]

Ющенко Альона Петрівна,
кандидат педагогічних наук, доцент,
доцент кафедри професійної освіти
Українського державного університету імені Михайла Драгоманова
https://orcid.org/0000-0002-0143-3663
e-mail: a.p.yushchenko@udu.edu.ua

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ У ВІЙСЬКОВІЙ СПРАВІ: ТЕОРЕТИЧНИЙ АСПЕКТ

У статті розглянуто теоретичні засади застосування криптографічних методів захисту інформації у військовій справі. Проаналізовано сутність та класифікацію криптографічних методів, їх роль у забезпеченні конфіденційності, цілісності та автентичності інформації в умовах сучасних воєнних конфліктів.

Наведено тлумачення терміна «криптографія» – наука про математичні методи й алгоритми перетворення повідомлення (відкритого тексту) на зашифрований (шифротекст), який неможливо прочитати без знання ключа або спеціального алгоритму.

Проведено порівняльну характеристику криптографічних методів, що застосовуються у військовій справі для захисту інформації. А також проаналізовано актуальні виклики, з якими стикаються військові під час використання криптографії.

Розглянуто ключові функції криптографії, зокрема: конфіденційність, цілісність, автентичність, незаперечність. Окрім цього, вказано, що криптографічні методи охоплюють усі сфери військових операцій, до яких належать такі, як: захист комунікацій; управління безпілотними системами; системи ідентифікації;захист збережених даних.

Особливу увагу приділено симетричним та асиметричним алгоритмам шифрування, криптографічним хеш-функціям, цифровому підпису та протоколам обміну ключами. Обґрунтовано значення криптографії як базового елементу системи інформаційної безпеки Збройних сил та інших військових формувань.

Зазначено, що у військовій справі вибір методу криптографічного захисту залежить від ієрархічного рівня передачі інформації: від стратегічного командування до тактичної ланки, а також потребує багаторівневого захисту.

Доведено, що військове планування розраховується на десятиліття вперед, оскільки актуальною є концепція «перехопити зараз – розшифрувати пізніше». Інакше кажучи, дані, які зашифровані сьогодні, можуть бути розшифровані через 10-15 років за допомогою квантових комп'ютерів.

Ключові слова: *криптографія, інформаційна безпека, військова справа, шифрування, криптографічні алгоритми, захист інформації.*

Інформація у військовій сфері завжди була стратегічним ресурсом від захищеності якого залежить ефективність управління військами, успішність операцій та безпека особового складу. В умовах цифровізації та активного використання інформаційно-комунікаційних технологій питання захисту військової інформації набуває особливої актуальності.

Повномасштабна збройна агресія російської федерації проти України суттєво посилила роль інформаційного та кіберпростору, як одного з ключових полів воєнних дій. Поряд із класичними видами збройної боротьби активно застосовуються кібероперації, радіоелектронна боротьба (РЕБ), інформаційно-психологічні впливи та спроби компрометації систем управління військами і критичної інфраструктури. За таких умов, правильний захист інформації стає не лише технічним інструментом, а й важливим чинником національної безпеки, що потребує постійного вивчення та вдосконалення.

Сучасні бойові дії в Україні характеризуються широким використанням автоматизованих систем управління, захищеного цифрового зв'язку, безпілотних літальних апаратів, супутникових технологій та мережевих платформ обміну даними. Усі ці елементи вимагають ефективного захисту для запобігання перехопленню, підміні або знищенню інформації противником.

Одним із ключових напрямів інформаційної безпеки є криптографія – наука, яка забезпечує конфіденційність, цілісність, автентичність і незаперечність інформації та виступає фундаментом для захисту каналів зв'язку, систем зберігання даних, процесів автентифікації. Саме тому теоретичне осмислення криптографічних методів захисту інформації у військовій справі набуває особливої цінності.

Метою статті є дослідження криптографічних методів, що застосовуються у військовій справі для захисту інформації, їх порівняльна характеристика, а також аналіз викликів, з якими стикається криптографія в умовах війни.

Криптографія (від грецького kryptós – прихований і gráphein – писати) – наука про математичні методи та алгоритми перетворення повідомлення (відкритого тексту) в зашифрований (шифротекст), який неможливо прочитати без знання ключа або спеціального алгоритму.

Основні функції криптографії:

1. Конфіденційність (інформація доступна лише уповноваженим особам);

2. Цілісність (неможливість зміни/ спотворення даних);

3. Автентичність (перевірка ідентичності користувача, пристрою, даних);

4. Незаперечність (неможливість відмови від авторства повідомлення).

Криптографічні методи класифікують за різними критеріями:

– типом ключа (симетричне шифрування, асиметричне, гібридні методи);

– способом перетворення та типом алгоритму (шифрування методом простої заміни, метод підстановки);

– типом даних (потокове шифрування, блочне, хешування) [1].

Симетричне шифрування передбачає використання одного ключа для шифрування й дешифрування (DES, AES, Blowfish, RC5). Переваги: висока швидкість, ефективність при обробці великих обсягів даних. Недоліки:

потребує безпечного обміну ключами.

DES (Data Encryption Standard). Розроблений у 1976 році компанією IBM, DES є одним із перших симетричних алгоритмів, офіційно прийнятим у США для захисту урядових даних. Довжина ключа становить 56 біт, що на сучасний момент вважається недостатньою через вразливість до атак повного перебору. DES використовує 16 раундів перетворень (Feistel network) для шифрування блоків даних розміром 64 біти.

AES (Advanced Encryption Standard). Використовується з ключами довжиною 128, 192 або 256 біт. AES є швидшим і безпечнішим за DES і широко застосовується в сучасних військових мережах.

Blowfish. Застосовується в системах, де потрібна гнучкість у розмірі ключа (до 448 біт).

RC5 – алгоритм шифрування, який використовує ключі змінної довжини до 2040 біт.

Асиметричне шифрування. Використовує пару ключів – відкритий (для шифрування) і закритий (для дешифрування). Переваги: не потребує попередньої передачі секретного ключа. Недоліки: нижча швидкість у порівнянні із симетричним шифруванням. Прикладами є такі ключі шифрування: RSA, ECC та Diffie-Hellman.

RSA (Rivest Shamir та Adleman). Базується на складності факторизації великих чисел. Використовується для обміну ключами та автентифікації.

ECC (Elliptic Curve Cryptography). Забезпечує високий рівень безпеки при меншій довжині ключа (наприклад, 256-бітний ключ ECC еквівалентний 3072-бітному RSA).

Diffie-Hellman. Використовується для безпечного обміну ключами через незахищені канали [5].

Гібридні методи шифрування. Поєднують обидва підходи: асиметричні методи використовуються для обміну ключами, а симетричні – для шифрування інформації.

За способом перетворення повідомлень в криптографії використовують шифрування методом простої заміни та шифр методом підстановки (зсуву).

Шифрування методом простої заміни полягає у створенні за певним алгоритмом таблиці шифрування, в якій для кожної букви відкритого тексту існує єдина зіставлена їй буква шифр-тексту чи шифр-числу. У цьому шифрі застосовуються числа, які замінюють літери. Щоб розшифрувати повідомлення отримувач повинен мати копію таблиці шифрування (ключ).

Шифр Цезаря (зсуву або підстановки) – алгоритм шифрування, в якому кожна буква відкритого тексту заміняється на ту, що віддалена від неї в алфавіті на сталу кількість позицій. Шифр названий на честь римського імператора Гая Юлія Цезаря, який використовував його для секретного листування зі своїми генералами з кроком зсуву «3». Наприклад, у шифрі із зсувом «3» літера А була б замінена на Г, Б – стане Д, і т.д.

Потокове шифрування – виконується по одному біту або байту (RC4, ChaCha). Переваги: придатне для реального часу.

RC4 (Rivest Cipher 4) є популярним та широко використовуваним алгоритмом потокового шифрування для захисту інтернет-трафіку (TLS) та даних в бездротових протоколах зв'язку (WEP та WPA).

ChaCha. Потоковий шифр, який забезпечує високу швидкість і стійкість до атак на слабкі ключі.

Блочне шифрування. Дані розбиваються на блоки фіксованого розміру, зазвичай 128 біт, кожен блок шифрується окремо (Serpent, IDEA).

Хешування. Хеш-функції використовуються для перевірки цілісності даних і створення цифрових підписів. Вони перетворюють дані довільної довжини в фіксований набір бітів (хеш) (SHA-2, BLAKE 2). Переваги: забезпечують швидку перевірку цілісності, стійкі до колізій (два різні повідомлення не повинні мати однаковий хеш), простота інтеграції в системи. Недоліки: не забезпечують конфіденційність, лише цілісність, уразливі до атак, якщо алгоритм застаріває (наприклад, SHA-1).

SHA-256/512 – широко застосовується для створення цифрових підписів і перевірки цілісності.

BLAKE 2 – швидший і безпечніший за SHA, використовується в системах із високими вимогами до продуктивності [5].

У військовій справі вибір методу криптографічного захисту залежить від ієрархічного рівня передачі інформації: від стратегічного командування до тактичної ланки і вимагає багаторівневого захисту. Цифрові технології базуються на жорсткій стандартизації. Це необхідно для забезпечення інтероперабельності (англ. interoperability – здатність до взаємодії), здатності різних підрозділів та союзників взаємодіяти між собою. Сьогодні основними векторами є стандарти США (як база для NATO) та національні стандарти України. Більшість військових протоколів Альянсу базуються на стандартах, розроблених або сертифікованих NIST (National Institute of Standards and Technology).

AES (Advanced Encryption Standard): на сьогодні є золотим стандартом для захисту тактичних даних. Його перевага у надзвичайній швидкодії на апаратному рівні. Сучасні військові процесори мають спеціальні набори інструкцій (наприклад, Intel AES-NI), що дозволяють шифрувати гігабіти інформації за секунду без перегріву обладнання.

Suite B та CNSA (Commercial National Security Algorithm Suite): набір алгоритмів, спеціально визначений Агентством національної безпеки США (NSA) для захисту інформації з грифом «Top Secret». Він включає використання еліптичних кривих для обміну ключами та алгоритми хешування сімейства SHA-384.

Україна має власний національний стандарт криптографічного захисту – «Калина». «Калина» (англ. Kalyna) – симетричний блочний шифр описаний у національному стандарті України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення». Національний стандарт набрав чинності з 1 липня 2015 року та розроблений у співпраці Державної служби спеціального

зв’язку та захисту інформації України і провідних українських науковців на основі проведення відкритого конкурсу криптографічних алгоритмів [3]. Розробка стандарту «Калина» була обумовлена необхідністю мати повний суверенітет у сфері захисту даних, що виключає можливість наявності «закладок» від іноземних виробників.

Ключові відмінності та переваги «Калини» порівняно з AES:

1. Збільшений розмір блоку: якщо AES оперує блоками по 128 біт, то «Калина» дозволяє використовувати блоки до 512 біт. Теоретично це забезпечує вищий рівень стійкості до складних методів лінійного та диференціального криптоаналізу.

2. Складніша структура перетворень (S-блоки): в українському стандарті використовується більша кількість таблиць замін, що суттєво ускладнює математичне моделювання атак на алгоритм.

3. Гнучкість: стандарт передбачає адаптацію під різні типи обчислювальних потужностей, що важливо для вітчизняних систем спеціального зв'язку.

Криптографічні методи захисту інформації (КМЗІ) у військовій справі еволюціонували від простих підстановок до складних ітеративних перетворень, що базуються на теорії чисел та абстрактній алгебрі. Теоретичний аспект захисту передбачає не лише вивчення алгоритмів, а й аналізі їхньої стійкості до детермінованих та імовірнісних методів криптоаналізу. На відміну від цивільного сектору, військова криптографія оперує поняттям «термін секретності». Якщо для банківської транзакції достатньо стійкості на кілька годин, то стратегічні плани вимагають захисту на десятиліття.

Симетричне шифрування залишається найефективнішим методом захисту військового зв'язку. Використання потокового шифрування критично важливо для передачі відео високої чіткості (Full HD/4K) з розвідувальних БПЛА або голосового зв'язку в реальному часі. Основною загрозою для БПЛА є «hijacking» (перехоплення керування) та GPS-spoofing (підміна координат).

Автентифікація команд: кожна команда, що надсилається з наземної станції керування (НСК), повинна мати унікальний криптографічний токен. Навіть якщо противник запише сигнал і спробує відтворити його пізніше (атака повторення), БПЛА відхилить таку команду, оскільки часовий штамп або лічильник циклів не співпаде.

Шифрування телеметрії: дані про стан апарата, його координати та заряд батареї шифруються швидкими потоковими шифрами, щоб ворог не міг визначити місцезнаходження оператора або маршрут повернення дрона [6].

Асиметрична криптографія вирішує головну проблему військової логістики: безпечний розподіл ключів. Використання пари «відкритий ключ/секретний ключ» дозволяє розгортати мережі зв'язку без попереднього фізичного обміну шифроблокнотами.

Цифрові підписи забезпечують автентичність наказів. У бойових умовах це гарантує, що команда на відкриття вогню або зміну дислокації надійшла саме від легітимного командування, а не від засобів РЕБ противника.

Управління ідентифікацією: Методи асиметричного шифрування лежать в основі систем розпізнавання «свій-чужий» (IFF – Identification Friend or Foe) в авіації та ППО.

Захист на рівні стратегічних магістралей. На цьому рівні використовуються найбільш стійкі методи. Основний акцент робиться на тунелюванні даних (VPN на апаратному рівні), де шифрується не тільки корисне навантаження, а й службова інформація пакетів (заголовки), щоб противник не міг провести аналіз трафіку та виявити структуру штабів.

Тактичні мережі MANET (Mobile Ad hoc Networks). Специфіка тактичного рівня – динамічність. Підрозділи постійно рухаються, зв'язок може зникати. Тут застосовуються методи динамічної перегенерації ключів. Якщо одна радіостанція потрапляє до рук ворога, система повинна автоматично виключити її з мережі та оновити криптографічні параметри для всіх інших учасників без переривання бою.

Цілісність даних у системах керування зброєю. Криптографія тут використовується не стільки для приховування даних, скільки для запобігання їх спотворенню. Наприклад, підміна координат цілі на кілька метрів може призвести до фатальних наслідків. Використання хеш-функцій дозволяє миттєво перевірити, чи не був пакет даних змінений під час передачі через незахищене середовище [2], [4].

Криптографічні методи охоплюють усі сфери військових операцій:

1. Захист комунікацій. Усі рівні командування – від тактичного до стратегічного використовують шифрування радіозв'язку, супутникових каналів, локальних мереж.

2. Управління безпілотними системами. Дрони та інші БПЛА потребують захищених каналів управління та передачі відео.

3. Системи ідентифікації. Криптографія лежить в основі систем «свій-чужий» (IFF – Identification Friend or Foe).

4. Захист збережених даних. Військові архіви, плани операцій, картографічна інформація – все шифрується та зберігається з використанням спеціалізованих алгоритмів.

Військове планування розраховується на десятиліття вперед. Існує концепція «перехопити зараз – розшифрувати пізніше» (Store Now – Decrypt Later). Це означає, що дані, зашифровані сьогодні, можуть бути розшифровані через 10-15 років за допомогою квантових комп'ютерів. Тому, подальші наукові дослідження у сфері криптографічного захисту інформації мають бути спрямовані на адаптацію теоретичних положень до практичних потреб Збройних сил України, а також на врахування специфіки сучасних воєнних конфліктів, що характеризуються поєднанням кінетичних і кібернетичних дій.

Використана література:

1. Бабаш А. В., Шанкіна Г. П. Криптографічні методи захисту інформації: підручник. Київ : Видавничий центр НУБіП України, 2019. 320 с.
2. Горбенко І. Д., Горбенко Ю. І. Криптографія та захист інформації в телекомунікаційних системах : підручник. Харків : ХНУРЕ, 2018. 412 с.
3. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. Введ. 01–07–2015. Київ : Мінекономрозвитку України, 2015.
4. Захист інформації в комп'ютерних системах і мережах : навч. посіб. / В. Г. Хорошко, С. І. Сидоренко, О. В. Поморова та ін. Київ : КНУ ім. Тараса Шевченка, 2020. 256 с.
5. Методи криптографічного захисту та автентифікації в мережах стільникового зв'язку військового призначення / Я. В. Зінченко, Я. Е. Курята, Р. Р. Лазута, В. Д. Могилевич, Ю. А. Крамська. *Наука і техніка*. 2025. № 5 (46). С. 1492-1502.
6. Козлов С. В., Іванов О. П. Сучасні методи аутентифікації в бездротових мережах військового призначення. *Вісник Військового інституту телекомунікацій та інформатизації*. 2023. № 2. С. 45-53.

References:

1. Babash A. V. & Shankina H. P. (2019). Kryptohrafichni metody zakhystu informatsii [Cryptographic methods of information protection]. Kyiv : Publishing center of NUBiP of Ukraine [in Ukrainian].
2. Horbenko I. D. & Horbenko Yu. I. (2018). Kryptohrafiia ta zakhyst informatsii v telekomunikatsiinykh systemakh [Cryptography and information security in telecommunication systems]. Kharkiv : HNURE [in Ukrainian].
3. DSTU 7624:2014. (2015). Information technology. Cryptographic protection of information. Symmetric block cipher algorithm. Ministry of Economic Development and Trade of Ukraine [in Ukrainian].
4. Khoroshko V. H., Sydorenko S. I., Pomorova O. V. et. al. (2020). Zakhyst informatsii v kompiuternykh systemakh i merezhakh [Information security in computer systems and networks]. Kyiv : Taras Shevchenko National University of Kyiv [in Ukrainian].
5. Zinchenko Ya. V., Kuriata Ya. E., Lazuta R. R., Mohylevych V. D., & Kramska Yu. A. (2025). Cryptographic protection and authentication methods in military cellular networks. *Science and Technology*. 5. P. 1492-1502 [in Ukrainian].
6. Kozlov S. V. & Ivanov O. P. (2023). Modern authentication methods in military wireless networks [Suchasni metody autentyfikatsii v bezdrotovykh merezhakh viiskovoho pryznachennia]. *Visnyk Viiskovoho instytutu telekomunikatsii ta informatyzatsii.* 2. P. 45-53 [in Ukrainian].

A. YUSHCHENKO. Cryptographic methods of information protection in military affairs: theoretical aspect.

he article considers the theoretical principles of the application of cryptographic methods of information protection in military affairs. The essence and classification of cryptographic methods, their role in ensuring the confidentiality, integrity and authenticity of information in the conditions of modern military conflicts are analyzed.

The interpretation of the term «cryptography» is given – the science of mathematical methods and algorithms for converting a message (plain text) into an encrypted (ciphertext) that cannot be read without knowing the key or a special algorithm.

A comparative characteristic of cryptographic methods used in military affairs to protect information is provided. And the current challenges that the military faces when using cryptography are also analyzed.

The key functions of cryptography are considered, in particular: confidentiality, integrity, authenticity, non-repudiation. In addition, it is indicated that cryptographic methods cover all areas of military operations, which include: communication protection; control of unmanned systems; identification systems; protection of stored data.

Particular attention is paid to symmetric and asymmetric encryption algorithms, cryptographic hash functions, digital signatures and key exchange protocols. The importance of cryptography as a basic element of the information security system of the Armed Forces and other military formations is

substantiated.

It is noted that in military affairs the choice of cryptographic protection method depends on the hierarchical level of information transmission: from strategic command to tactical level, and also requires multi-level protection.

It is proved that military planning is calculated for decades ahead, since the concept of «intercept now – decrypt later» is relevant. In other words, data encrypted today can be decrypted in 10-15 years using quantum computers.

Key words: *cryptography, information security, military affairs, encryption, cryptographic algorithms, Data Security.*

Дата першого надходження рукопису до видання: 10.12.2025

Дата прийнятого до друку рукопису після рецензування: 24.01.2026

Дата публікації: 06.02.2026