Секція 1

## ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ШИФРУВАННЯ ДАНИХ

Абрамова В. Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Брежнєв Є. В.

**Актуальність** порівняльного аналізу методів шифрування даних зберігається через постійний розвиток технологій і необхідність забезпечення безпеки інформації та захисту від нових загроз. Кіберзагрози та методи злому вимагають від методів шифрування адаптації до нових умов. Комплексна система захисту інформації вимагає виявлення раціональної комбінації методів захисту для зниження ризиків кібербезпеки.

**Метою** порівняльного аналізу методів шифрування даних є виявлення відповідного методу для забезпечення необхідного рівня захисту інформації при оптимальній потужності та дотриманням вимог безпеки.

**Основні положення.** Існує декілька основних методів шифрування даних які мають свої переваги та недоліки. Симетричне шифрування – це метод, коли один ключ використовується як для шифрування, так і для розшифрування даних [1]. Перевага метода – швидке шифрування, тож він підходить для роботи з великим обсягом інформації. Недоліком є необхідність вирішення проблеми безпечної передачі ключа та неможливість використовування в ЕЦП через відомість ключа для обох сторін. Приклади: AES (Advanced Encryption Standard), DES (Data Encryption Standard). Асиметричне шифрування – для шифрування даних використовують відкритий ключ, а для розшифровування – закритий [2]. Розшифрування відбувається тільки за допомогою закритого ключа. Цей ключ не може бути визначеним з ключа зашифровування. Перевагою є забезпечення високого рівня безпеки та зручність обміну ключами, але при роботі з невеликим обсягом даних – є менш продуктивним. Приклади: RSA, ECC. Хешування – перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини (хеш-функцію) [3]. Використовується тільки для перевірки цілісності даних через необоротність перетворення. Приклади: SHA-256, MD5. Гібридне шифрування – комбінація симетричного та асиметричного шифрування для забезпечення безпеки обміну ключами та ефективності шифрування [4]. Симетричний ключ використовується для шифрування даних, а асиметричний для шифрування самого симетричного ключа. Недолік - Може вимагати більше обчислювальних ресурсів. Квантове шифрування – цей метод використовується для передачі ключа симетричного шифрування [5]. Він заснований на принципах квантової фізики, що забезпечує високий рівень захисту від злому за допомогою квантових

обчислень. Перевагою методу є можливість виявлення втручання до процесу квантового розподілу ключа, але на даний час передача неможлива на великі відстані.

В роботі виконаний порівняльний аналіз таких методів шифрування даних: AES, DES, RSA, ECC SHA-256, MD5, гібридне шифрування, квантове шифрування. Були висвітлені їх переваги, недоліки та принципи використання.

**Висновки.** Розвиток технологій зумовлює збільшення обсягів оброблюваних даних, які треба захистити та появу нових методів шифрування. Отже, порівняльний аналіз методів шифрування даних залишається вкрай важливими для підтримки безпеки інформації, захисту від нових загроз та підтримання актуальності в галузі криптографії. Для вибору необхідного методу шифрування пропонується використовувати їх показники щодо рівня безпеки, швидкості роботи, контексту застосування та дотримання галузевих стандартів та нормативних вимог.

**Список літератури**

1. Hlynchuk L., Hryshanovych T., Stupin A. (2021). Реалізація стандарту симетричного шифрування DES мовою програмування C та порівняння часу його роботи з відомими утилітами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(14), 118–130. DOI: https://doi.org/10.28925/2663-4023.2021.14.118130;
2. Що таке шифрування та як воно працює? *Kingston Technology*. URL: https://www.kingston.com/ua/blog/data-security/what-is-encryption (дата звернення: 10.11.2023);
3. Hash функції. *Medium*. URL: https://medium.com/techmaker/hash-функції-90bf2be2af1e (дата звернення: 09.11.2023);
4. Воробйов В.Г. Теоретичні основи побудови гібридних криптографічних систем захисту інформації. Сучасні Інформаційні Технології / 4. Інформаційна безпека. URL: https://www.rusnauka.com/18_NPRT_2017/Informatica/4_227128.doc.htm (дата звернення: 10.11.2023);
5. Квантова криптографія. *Енциклопедія сучасної України*. URL: https://esu.com.ua/article-11921 (дата звернення: 11.11.2023);

**Відомості про авторів**

Абрамова Валерія Денисівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», v.d.abramova@student.csn.khai.edu
Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., старший науковий співробітник, e.brezhnev@csn.khai.edu