УДК 004.056+511.176

# ПРО МОЖЛИВІСТЬ ЗАБЕЗПЕЧЕННЯ АВТЕНТИФІКАЦІЇ ПІДВИЩЕНОЇ СТІЙКОСТІ

**Яремчук Юрій,** д.т.н., професор, директор Центру інформаційних технологій і захисту інформації.

**Салієва Ольга,** аспірант кафедри менеджменту та безпеки інформаційних систем.

Вінницький національний технічний університет, Україна

На сьогодні вирішення проблеми цілісності інформації є не менш важливою, ніж проблема вирішення її конфіденційності [1]. Якщо конфіденційність забезпечується за допомогою криптосистем, то для вирішення проблеми цілісності інформації застосовують криптографічні протоколи, найбільш поширеними з яких є криптографічні протоколи автентифікації та цифрового підписування [2]. У загальному вигляді в схемі автентифікації сторін взаємодії існує два учасника [1]: претендент (сторона, яка повинна довести свою автентичність) та перевіряльник (сторона, яка цю автентичність повинна перевірити). Претендент має два ключа – загальнодоступний $K_1$ та секретний $K_2$. При доведенні автентичності з нульовим розголошенням претенденту необхідно довести, що він знає $K_2$, причому зробити це таким чином, щоб це доведення можна було б перевірити знаючи лише $K_1$.

Теоретичні основи схем автентифікації було закладено у відомій роботі Сіммонса [3]. Найбільш відомими методами автентифікації є методи Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра [1]. Ці методи базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації. Крім того актуальним залишається підвищення стійкості схем автентифікації.

В цьому зв’язку певний інтерес викликає математичний апарат на основі рекурентних послідовностей, який дозволяє за певних умов спрощувати обчислення під час вирішення криптографічних задач. Так у роботах Яремчука Ю.Є [4-6] представлено методи автентифікації сторін взаємодії, які базуються на рекурентних $V_k$ та $U_k$–послідовностях і які, у порівнянні з відомим методами, дозволяють суттєво спрощувати обчислення.

Проведено дослідження і запропоновано модифікацію методів на основі $V_k$ та $U_k$–послідовностей, яка забезпечує автентифікацію сторін взаємодії підвищеної стійкості.

Проведено аналіз, який показав, що криптографічна стійкість запропонованої модифікації методу автентифікації є вищою, ніж відомих аналогів, а обчислювальна складність запропонованого методу в цілому має приблизно такий же рівень складності обчислень, що й відомого аналогу.

Це досягається за рахунок необхідності претенденту передавати дещо більшу кількість чисел і виконувати три обчислення елементів $V_k$–послідовності за прискореним алгоритмом, замість двох як у відомому методі. Однак, за рахунок зменшення обчислювальної складності процедури перевірки автентичності у запропонованій модифікації методів на основі $V_k$ та $U_k$–послідовностей забезпечується у цілому приблизно такий же рівень обчислювальної складності, що і у відомих методах.

**Список використаної літератури**


1. Menezes A. J. Handbook of Applied Cryptography // Menezes A. J., van Oorschot P. C., Vanstone S. A.. – CRC Press, 2016. – 816 p.
2. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия–Телеком, 2007. – 320 с.
3. Simmons G. J., Authentication theory/coding theory // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – V. 196, 1985. – Pp. 411–431.
4. Яремчук Ю.Є. Методи автентифікації на основі рекурентних послідовностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1(25), 2013. – С. 39–49.
5. Яремчук Ю.Є. Метод автентифікації суб'єктів (об'єктів) взаємодії на основі рекурентних послідовностей // Вісник Вінницького політехнічного інституту. – №3, 2013. – С. 99–104.
6. Яремчук Ю.Є. Метод автентифікації учасників взаємодії на основі рекурентних послідовностей // Реєстрація, зберігання і обробка даних. – Т. 15, №2, 2013. – С. 73–81.