УДК 004.056.55:378.147

**О. М. Палій**
**І. М. Кобилянська**

# ПРОБЛЕМНО-ОРІЄНТОВАНИЙ ПІДХІД ЩОДО ВИКЛАДАННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Вінницький національний технічний університет

***Анотація.*** *У тезах розглядається можливість використання проблемно-орієнтованого підходу (PBL) у викладанні методів захисту інформації у закладах вищої освіти. Схеми порогового розподілу секрету запропоновано як модельну навчальну задачу, що поєднує математичну строгість з практичною мотивацією. Показано, яким чином конструкції на основі узагальнених послідовностей Фібоначчі можуть слугувати прикладом для формування фахових компетентностей студентів спеціальності «Кібербезпека».*

**Ключові слова:** проблемно-орієнтоване навчання, розподіл секрету, захист інформації, узагальнені послідовності Фібоначчі, педагогічні технології.

***Abstract.*** *The theses examine the potential of applying a problem-based learning (PBL) approach to teaching information security methods in higher education institutions. Threshold secret sharing schemes are proposed as a model learning task that combines mathematical rigor with practical motivation. It is shown how constructions based on generalized Fibonacci sequences can serve as an example for developing professional competencies of students majoring in Cybersecurity.*

**Key words:** problem-based learning, secret sharing, information security, generalized Fibonacci sequences, pedagogical technologies.

## Вступ

Підготовка фахівців з кібербезпеки вимагає не лише передачі теоретичних знань, а й формування здатності аналізувати та розв'язувати нетривіальні прикладні задачі. Одним із сучасних підходів до організації навчального процесу у закладах вищої освіти є проблемно-орієнтоване навчання (Problem-Based Learning, PBL) − метод, за якого студенти здобувають знання в процесі вирішення реальних або змодельованих проблем [1]. Ефективність PBL у технічних дисциплінах підтверджена численними дослідженнями [2]. Водночас вибір навчальної задачі є ключовим чинником успіху: вона має бути достатньо складною, щоб стимулювати пошук, і водночас доступною для студентів відповідного рівня підготовки.

У даній роботі пропонується використовувати схеми порогового розподілу секрету − зокрема, конструкції на основі узагальнених послідовностей Фібоначчі − як модельну задачу в курсах захисту інформації та прикладної криптографії.

## Результати дослідження

Схеми порогового розподілу секрету є фундаментальним поняттям криптографії: за схемою (t, n) секретне значення s розподіляється між n учасниками таким чином, що будь-яка підмножина з t учасників може відновити s, тоді як будь-яка підмножина меншого розміру не отримує про нього жодної інформації [3]. Класична конструкція Шаміра базується на поліноміальній інтерполяції над скінченним полем [4].

Авторська пропозиція полягає у використанні узагальнених послідовностей Фібоначчі як альтернативного математичного базису для побудови порогових схем. Рекурентне співвідношення виду $F(n) = c_1 \cdot F(n-1) + c_2 \cdot F(n-2) + \ldots + c_k \cdot F(n-k)$ задає клас числових послідовностей із багатою структурою, що відкриває нові конструктивні можливості [5]. Така конструкція нетривіальна математично, проте допускає поступове введення: від простих прикладів (послідовність Фібоначчі) до загального випадку.

З педагогічної точки зору, ця задача є ефективною для PBL з кількох причин:
По-перше, задача має чітке практичне формулювання: «як безпечно розподілити ключ між учасниками системи?» − що одразу мотивує студентів.

По-друге, вона охоплює широкий спектр математичних понять: теорія чисел, лінійна алгебра, скінченні поля, рекурентні послідовності, − що забезпечує міждисциплінарну інтеграцію.

По-третє, задача має природне масштабування складності: від аналізу класичної схеми Шаміра до самостійної побудови та аналізу нових конструкцій на основі Фібоначчі-узагальнень, що дозволяє диференціювати навантаження для різних рівнів підготовки.

Запропонована методична схема включає такі етапи: (1) постановка проблеми − наведення реального сценарію розподіленого зберігання ключа; (2) самостійне вивчення базової теорії; (3) аналіз класичного рішення (Шамір); (4) дослідницький етап − побудова альтернативної схеми на основі узагальненої послідовності Фібоначчі; (5) перевірка коректності та безпеки побудованої схеми; (6) презентація та захист результатів.

## Висновки

Схеми порогового розподілу секрету на основі узагальнених послідовностей Фібоначчі є перспективною навчальною задачею для проблемно-орієнтованого навчання в курсах захисту інформації. Така задача поєднує практичну мотивацію, математичну глибину та можливість масштабування складності, що відповідає вимогам сучасних педагогічних технологій в закладах вищої освіти. Подальші дослідження планується спрямувати на розробку та апробацію повноцінного навчального модуля на основі запропонованого підходу.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Hmelo-Silver C. E. Problem-Based Learning: What and How Do Students Learn? Educational Psychology Review. 2004. Vol. 16, No. 3. P. 235–266.
2. Prince M. Does Active Learning Work? A Review of the Research. Journal of Engineering Education. 2004. Vol. 93, No. 3. P. 223–231.
3. Beimel A. Secret-sharing schemes: a survey. Coding and Cryptology: Third International Workshop, IWCC 2011. Springer, 2011. P. 11–46.
4. Shamir A. How to share a secret? Communications of the ACM. 1979. Vol. 22, No. 11. P. 612–613.
5. Stakhov A. P. The generalized golden proportions, a new theory of real numbers, and ternary mirror-symmetrical arithmetic. Chaos, Solitons & Fractals. 2007. Vol. 33, No. 2. P. 315–334.



***Палій Олексій Миколайович –*** *аспірант групи F5-25a, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: alexey.paliy1337@gmail.com.*

***Кобилянська Ірина Миколаївна*** *– кандидат педагогічних наук, доцент, викладач кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: irishakobilanska@gmail.com.*

***Oleksii Palii*** *– postgraduate student of group F5-25a, Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, Email: alexey.paliy1337@gmail.com.*

***Iryna Kobylianska*** *– Candidate of Pedagogical Sciences, Associate Professor, Lecturer of the Department of Life Safety and Safety Pedagogy, Vinnytsia National Technical University, Vinnytsia, Email: irishakobilanska@gmail.com.*