УДК 004.056.55

**А. О. Душко**
**Ю. В. Баришев**

# ЗАСІБ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ НА ОСНОВІ ПСЕВДОНЕДЕТЕРМІНОВАНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Вінницький національний технічний університет

***Анотація***

*Проаналізовано застосування псевдонедетермінованих криптографічних перетворень, щодо можливості їх використання у засобах захищеного обміну даними. Запропоновано новий засіб захищеного обміну даними, робота якого дозволятиме користувачам обмінюватися різними даними (файлами) з іншими користувачами.*

**Ключові слова:** псевдонедетермінований, криптографічні перетворення, передавання даних, алгоритм.

***Abstract***

*The use of pseudonondeterministic cryptographic transformations is analyzed, as to the possibility of their use in secure data exchange. A new secure data exchange tool is proposed it will allow users to share different data (files) with other users.*

**Keywords:** pseudonondeterministic, cryptographic transformations, data transmission, algorithm.

## Вступ

Основною небезпекою при передачі файлів між користувачами є пошкодження їх цілісності, втрата частини даних, підміна або ж затримка в їх отриманні іншою стороною передачі. В результаті користувач, при отриманні такого файлу, може отримати недостовірну інформацію. Використання таких даних є небезпечним перш за все для нього, а потім вже для інших користувачів, яким він передає ці дані. Така інформація може містити різного роду помилки, що можуть призвести до відмови середовища де вони використовуються. Саме тому актуальність розробки засобів захищеного обміну даними полягає в можливості вирішити проблему незахищеного передавання файлів між користувачами в режимі реального часу. Використання псевдонедетермінованих криптографічних перетворень дозволить зробити даний засіб надійним, а файли, що передаватимуть користувачі за допомогою нього, будуть захищеними від пошкодження їх цілісності.

Метою даного дослідження є підвищення захищеності файлів при їх передачі між користувачами за допомогою використання псевдонедетермінованих криптографічних перетворень.

Для досягнення мети необхідно розв’язати такі задачі:

- проаналізувати відомі засоби захищеного обміну даними;
- проаналізувати використання псевдонедетермінованих криптографічних перетворень;
- проаналізувати доцільність розробки захищеного засобу передачі даних на основі псевдонедетермінованих криптографічних перетворень.

## Аналіз методів забезпечення захищеного обміну даними

Захист інформації тією чи іншою мірою має забезпечуватися будь-якою системою обміну даними [1]. При цьому впорядкування та консолідація інформації, впорядкування даних та файлів дає можливість створити більш якісну систему захисту.

Величезне значення для забезпечення конфіденційності інформації мають криптографічні системи захисту даних [2]. Їх застосування забезпечує конфіденційність даних навіть у разі їх потрапляння до рук сторонньої особи. Але не варто забувати, що будь-який криптографічний алгоритм має таку властивість як криптостійкість, тобто і його захист має певну межу. Немає шифрів, які не можна було б зламати — це лише питання часу і коштів. Ті алгоритми, які ще кілька років тому вважалися надійними, сьогодні вже можуть бути скомпрометованими. Але використання таких методів захисту

для засобів захищеного обміну даними між користувачами, яким просто потрібно передати інформацію у нормальному та достовірному вигляді, є одним із найкращих методів.

На сьогодні основним і практично єдиним із запропонованих на ринку рішенням для забезпечення достовірності відправника файлу є електронно-цифровий підпис (ЕЦП) [3]. Основний принцип роботи ЕЦП заснований на використанні стандартів шифрування за допомогою відкритого ключа. Слід зауважити, що ключі для шифрування і розшифрування даних різні. Є закритий ключ, який дозволяє шифрувати інформацію, він зберігається тільки у власника, а є відкритий ключ, за допомогою якого можна перевірити справжність підпису, отриманого листа, файлу, він може поширюватися публічно. При підтвердженні достовірності відправника файлу, дані, що будуть отримані від нього, є цілісними та представлені у такому вигляді як їх і відправляли. Але завжди є можливість того, що той хто буде відправляти файл може навмисно надати неправильну інформацію. В такому випадку користувач ніякими засобами захисту не буде застрахований від тих даних, що він отримав. До того ж, учасники обміну даними, при неправильній реалізації ЕЦП, можуть ненавмисно пошкодити файли, що передаються.

Також, один із методів захищеного обміну інформацією є протоколювання [4]. Даний метод забезпечить однаковий спосіб передачі інформації і обробки помилок при взаємодії різного програмного забезпечення на основі певної апаратної платформи, що з'єднана з тим чи іншим інтерфейсом.

Одним з напрямів розвитку методів захисту обміну даними є псевдонедетерміноване шифрування. Особливістю концепції псевдонедетермінованої криптографії є те, що методи криптографічних перетворень виглядають для зловмисника як такі, що виконуються за допомогою недетермінованого автомата [5]. Недетермінованим вважається такий автомат, в якого правила переходу не обов'язково є функцією. Тобто, з одного початкового стану $s_0$ при реакції на одні й ті самі вхідні дані автомат може перейти в декілька різних станів [6].

Нехай ε – порожнє повідомлення, тоді недетермінований автомат описується у вигляді п'ятірки $\{S, A, \delta', s_0, D\}$, де $\delta'$ – відображення $S \times (A \cup \{\varepsilon\}) \to S$, де S – множина станів автомата; A – вхідний алфавіт; $s_0$ – виокремлений стан автомата, що називається початковим ($s_0 \in S$ ); D – підмножина в S, що називається множиною завершальних станів. Таким чином, поняття псевдонедетермінованого криптографічного перетворення, аналогічно до поняття псевдовипадкових чисел, передбачає, що дане перетворення для стороннього спостерігача (зловмисника) має такий вигляд, наче воно виконується недетермінованим автоматом. Однак для спостерігача, який знає правило-ключ дане перетворення виглядає, як таке, що виконується детермінованим автоматом. З наведених вище визначень випливає, що дана задача розв'язується шляхом заміни відображення $\delta$ , яке є однозначним, тобто $\delta$ – функція, на відображення $\delta'$ , яке не обов'язково є однозначним.

## Структура засобу захищеного обміну даними

З аналізу вище наведеного опису засобів захищеного обміну даними та псевдонедетермінованих криптографічних перетворень випливає, що доцільність розробки засобу, який складається з таких модулів:

- модуль авторизації користувачів;
- модуль автентифікації учасників обміну;
- модуль передавання даних;
- модуль криптографічного захисту даних.

Ключовим елементом для реалізації даного засобу стане запропонований підхід до криптографічних перетворень. Даний спосіб передбачає керований підхід до вибору однієї з множини функцій, при цьому на кожній з її ітерацій залишаючи сталість аргументів, що з точки зору криптографічної стійкості є важливою властивістю.

Модуль криптографічного захисту повинен передбачати такі алгоритми:

- блокове шифрування – для можливості передавання файлів;
- потокове шифрування – для можливості забезпечення зв'язку між користувачами в режимі реального часу.

Такий засіб дозволить користувачам не тільки передати у нормальному вигляді файли, але й зберегти їх цілісність та достовірність інформації, що в них знаходиться.

## Висновки

Застосування псевдонедетермінованих криптографічних перетворень при розробці та реалізації засобу захищеного передавання даних дозволяє досягти підвищеної захищеності файлів при їх передачі між користувачами. Для збільшення стійкості при передачі файлів псевдонедетерміновані криптографічні перетворення будуть виконувати роль захисту для даних, файлів та інформації що передаються. Реалізація даного засобу дозволить користувачам легко та безпечно обмінюватися будь-якою інформацію, при цьому не буде втрачатися її цілісність та достовірність, що є головною ознакою таких засобів.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Петров А.А. Компьютерная безопасность / Петров А.А. – Москва: Лайт Лтд., 2000 – 448 с.
2. Нильс Фергюсон, Брюс Шнайер. Практическая криптография / Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : Диалектика, 2004. — 432 с. — 3000 экз.
3. Лужецький В. А. Захист персональних даних: навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв. – Вінниця: ВНТУ, 2009. – 487 ст.
4. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. — СПб.: Питер, 2003. — с. 83-93 — (Серия «Классика computer science»).
5. Luzhetsky V. The Generalized Construction of pseudonondeterministic hashing / Volodymyr Luzhetsky, Yurii Baryshev// Computing, – 2012 – Vol. 11. Issue 3 – P. 302-308.
6. Баришев Ю. Структури операційних пристроїв для реалізації псевдонедетермінованих криптографічних перетворень / Юрій Баришев // Матеріали Міжнародної науково-практичної конференції "Інформаційні технології та комп'ютерне моделювання", м. Івано-Франківськ, 23-28 травня 2016 року. – Івано-Франківськ: Супрун В. П., 2016 – С. 109-110.



***Душко Аліна Олександрівна*** – студент, факультет інформаційних технологій та компютерної інженерії, Вінницький національний технічний університет, Вінниця, email: dushko483@gmail.com.

***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, email: yuriy.baryshev@vntu.edu.ua.

***Dushko Alina*** – student, Faculty of Information Technology and Computer Engineering, Vinnytsa National Technical University, Vinnytsia, email: dushko483@gmail.com.

***Baryshev Yurii*** – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, email: yuriy.baryshev@vntu.edu.ua.