УДК 004.52

Вторук О.В.
Савицька Л.А.
Добровольська Н.В.

РОЗРОБКА БЕСПЕЧНОГО ОРГАНАЙЗЕРА З АУДІОСПОВІЩЕННЯМ ДЛЯ НАВЧАННЯ

Вінницькій національний технічний університет

Анотація
Розроблено безпечний органайзер з аудіосповіщеннями для навчання. Використано шифрування AES256 та генератор псевдовипадкових чисел HMACSHA1, який використовує хеш функцію SHA1 та сіль для генерації ключа.
Ключові слова: шифрування, AES-256, органайзер.

Abstract
Developed a secure organizer with audio alerts for learning. AES256 encryption and the HMACSHA1 pseudo-random number generator, which uses the SHA1 hash function and salt to generate the key, were used.
Keywords: encryption, AES-256, organizer

У нас все більше справ і ми нерідко забуваємо щось зробити. Для цього людство придумало безліч методів [1]. В давнину в римі були раби, котрі нагадували своїм хазяїнам про важливі справи. Пізніше люди почали робити замітки у блокнотах та щоденниках. Ще пізніше до нас прийшли стікери, якими обліплювали все, від робочого столу до холодильника. А зараз, у часи комп'ютерної ери, є цифрові нагадувачі, органайзери, які допоможуть не забути про свій графік та важливі справи.

Для сучасного органайзера дуже важливо не потонути в потоці "сміттєвих" сповіщень, які йдуть нам від месенджерів, імейлів, все можливих додатків та іншого. Нерідко важливі сповіщення просто губляться в какофонії звуків та повідомлень. Тому варто використовувати сповіщення Windows та аудіо користувача, котрі проґавити куди важче.

Дуже важливо, в даному питанні залишатися приватним. Зазвичай люди не діляться своїми планами з незнайомцями, а є такі справи в які не варто посвячувати і рідних. Тому варто додати шифрування та вхід по паролю до органайзеру і ми отримаємо захищений планувальник подій.

Використання тотального шифрування даних забезпечує відносно високу надійність, а продуманий алгоритм сповіщень забезпечує підвищену увагу до самих сповіщень. Для шифрування даних [2] використовується алгоритм AES з 256 бітним ключем. Для перетворення паролю в ключ використовується генератор псевдовипадкових чисел HMACSHA1. Алгоритм передбачає як відсутність користувача біля ПК в момент сповіщення так і запуск програми з нагромадженим списком сповіщень. Таким чином даний органайзер забезпечує дві основні функції – безпеку та нагадування. Проте використання тотального шифрування призводить до того, що у випалку втрати паролю з якого генерується ключ шифрування втрачається і доступ до всіх даних програми.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Meyer, Bertrand (1997). Object-Oriented Software Construction. Prentice Hall. ISBN 0-13-629155-4.
2. Luzhetsky, V., Savitskaya, L.Development and research of adaptive data compression methods based on linear fibonacci form Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2015, 1(9), стр. 16–22

Вторук Олександр Володимирович- студент групи 1КІ-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vtoruk02@gmail.com

Савицька Людмила Анатоліївна – доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця, e-mail: **savytska.liudmyla@vntu.edu.ua**

Добровольська Наталія Вікторівна – доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця, e-mail: natali0212@ukr.net

Vtoruk Oleksandr - student of group 1KI-18b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vtoruk02@gmai.com

Savytska Liudmyla - Associate Professor of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: **savytska.liudmyla@vntu.edu.ua**

Dobrovolska Nataliia - Associate Professor of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: