Intellectual System Backup and Encrypt Information

Bohdan Tataryn, Taras Basyuk, Taras Batiuk

Lviv Polytechnic National University, Lviv, Ukraine

Physical storage media, no matter it is a flash drive, CD / DVD drives, hard drive or solid state drive, have the unpleasant property of failure, and flash drives are still lost. And, as a rule, the device fails at the most inopportune time. For a student, it can be the eve of passing a course work or diploma, for a programmer - a demonstration of the work of an important project, for the marketer hours and nerves, spent on the development of an advertising campaign, etc., each decides independently what information is important to him, and what can be risked. What is most interesting is that we are aware of the importance of lost information after it has been lost, although this is not only true of information. In fact, it took time to create a particular file, or some of the information, and time was known to be money. So, at a subconscious level, we are afraid of losing money. Moreover, the second time may not be: a photographer who has been sitting for more than one day in an ambush, will not be able to photograph a rare animal a second time, the student may have a chance to re-diploma, but not this year, and the marketer will have to look for another job after as customers of the advertising campaign turn to competitors.

Given this, it is important to create a system that helps its users to back up their information. This would greatly simplify the lives of those who possess important information, the loss of which would be a major problem for them.

References

1. Centralized secure backup system and method. - Access mode: https://patentimages.storage.googleapis.com/37/2d/09/338375715b9383/US6574733.pdf
2. Encryption of data to be stored in an information processing system. - Access mode: https://patents.google.com/patent/US8024582B2/en
3. A cryptographic file system.- Access Mode: https://www.umj.com.ua/article/5941/
4. Vambol, A.: The Matrix-based Knapsack Cipher in the Context of Additively Homomorphic Encryption. In: Computational linguistics and intelligent systems, 344-354. (2019)
5. Lytvyn, V., Peleshchak, I., Peleshchak, R., Vysotska, V.: Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm. In: 3rd International Conference on Advanced Information and Communications Technologies, AICT, 447-450. (2019)
6. Chyrun, L., Chyrun, L., Kis, Y., Rybak, L.: Automated Information System for Connection to the Access Point with Encryption WPA2 Enterprise. In: Lecture Notes in Computational Intelligence and Decision Making, 1020, 389-404. (2020)
7. Nazarkevych, M., Oliarnyk, R., Troyan, O., Nazarkevych, H.: Data protection based on encryption using Ateb-functions. In: 2016 XIth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT), 30-32. (2016)