31. **Denys Stolbov**

Visual models of cipher algorithms for students' learning information security

Our long-term experience of teaching students the basics of information security shows that a cryptography as a chapter of this course is not easy to learn. The students have problems with understanding some encryption algorithms, especially their complicated mathematical tools. On the other hand, it is quite difficult for a teacher to explain for students main features of structure and functionality such algorithms. At the same time, it has been found experimentally that visual information is perceived and remembered by a person better than text, sound and tactile. All this stimulated us to develop special dynamic computer models to visualize several cipher algorithms. In our study we represent the models, which describe and demonstrate the main stages of the public key (asymmetry) encryption algorithms. Firstly, in one of our models we rendered a mechanism of generation a pair of algorithm's keys and a procedure of their exchange between a sender and a receiver. Secondly, we paid attention to the visualization of RSA algorithm. An asymmetry of this algorithm is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. Our implemented computer model of RSA algorithm allows to present complicated mathematical idea of the factoring problem in a simple, understandable and accessible form for the students. The models were implemented by us in dynamic mathematics software GeoGebra that is open source with powerful tools for quickly and easily created of computer mathematical models.