Д.О. Васяева
Научный руководитель: ст. преподаватель О.А. Фролова
Муромский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
Владимирская обл., г. Муром, ул. Орловская, д. 23
E-mail: v-dasha95@yandex.ru

Comparative Analysis of Cryptographic Virtual Laboratory

Cryptography, or cryptology, is the practice and study of techniques for secure communication in the presence of the third parties called adversaries. [1]

The purpose of the cryptographic system is to encrypt a meaningful original text (also called “a clear text”) and get a completely meaningless at first glance ciphertext as a result. The recipient, whom it is intended for, should be able to decrypt the ciphertext restoring this into the original.

In accordance with state standards, a physical cryptographic laboratory should include a hardware computing department equipped with a certain kind of computer equipment connected to the local area network and the Internet, academic network software and training software, as well as an information security software and hardware department equipped with anti-virus software systems, hardware user authentication tools, hardware and software for protection of information (including cryptographic protection of information). [2]

As it can be seen, the study of cryptography requires a large amount of equipment, which in its turn requires high costs. As a rule, not all schools can afford to create a full physical cryptographic lab, so we came to the idea that it is possible to create a virtual cryptographic laboratory.

Unlike virtual physics laboratory, a virtual one requires much less material costs, which would allow educational institutions to spend their budget on other equally important goals. This is one of the main ideas of this paper.

To use a virtual cryptographic laboratory, we only need a personal computer or a laptop. All cryptography and related processes will be modeled on a running machine.

Students will be able to work on projects outside the institute, which should increase the speed of performing tasks as everything they need is always available at any time.

This laboratory will also make a full report on the course of work at the end of different processes which in its turn will help students prepare documentation to hand in.

Cryptography today is the most important part of all information systems: from email to mobile, from access to the Internet to electronic cash. And in the future, as commerce and communications are all closely connected to computer networks, cryptography will become an integral part of our lives. Therefore, we must promote the development of the learning process, and we hope that development of a cryptographic virtual laboratory will be one of the steps on this path.

Литература

1. Bulatova M.B. Cryptographic means of information protection // Режим доступа: http://www.rusnauka.com/15_NNM_2014/Informatica/1_170119.doc.htm.

2. Demchenko Yu.V., Petrenko A.I. Development of Instructional Methodology for Teaching Computer Networking and Information Resource Management Technologies in Kiev Polytechnic Institute // Режим доступа: http://www.uazone.org/demch/papers/jenc7.htm.