minimum number of scans required to meet compliance requirements. However, more frequent scanning (e.g. weekly) provides several benefits:

The acting phase of the vulnerability management program uses the data generated from previous phases to improve program. Changes may apply to company security policies, practices and procedures. These changes may result in organizational risk reduction, increased process efficiency and improved regulatory compliance. Common areas of improvement, as outlined in [4].

**References**

1. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.

2. Shanks W. Building a Vulnerability Management Program – A project management approach. SANS Institute, 2013.

3. Foreman P. Vulnerability Management. Auerbach Publications, 2009.

4. Manzuik S., Pfeil K., Gold A. Network Security Assessment: From Vulnerability to Patch. Syngress Media, 2006.

## PROTECTION OF SPEECH INFORMATION DURING TRANSMISSION VIA MOBILE NETWORKS

Khomo Khoaba Bigde, E.A. Ogorodnikov, O.B. Zelmanski

With the growing importance of the telecommunication systems and internet, secure transmission of information is crucial [1]. Cryptography helps in providing this much needed data confidentiality by converting data into an unrecognizable form. The decryption techniques allows intended receiver to reveal the contents of previously encrypted data via secrete keys exchanged exclusively between transmitter and receiver. The encryption and decryption techniques can be applied equally to a data in any form such as text, image, audio or video.

In this research the protection of speech information during transmission via mobile networks was focused on. A voice encryption and decryption system was programmed as a real-time software application. C# programming language was used. The NAudio class library, which is an open-source library for controlling audio on Windows-based computers was also applied and evaluated. It can be used with .NET applications using a variety of languages, for the protection of speech (audio) signals the TripleDES algorithm was used.

The software application is based on the following algorithm. The original audio signal is loaded to the wave viewer software and played by a speaker system. The data loaded and displayed on the wave viewer is encrypted and the results as a wave format are stored. After this the encrypted audio is loaded to the wave viewer software, played and recorded by the microphone of another personal computer or a phone. Then the recorded encrypted audio is decrypted to the original audio and played.

**Literature**

1. Study of the relationship of signal/noise ratio and speech intelligibility in possible points of information leakage / Amakiri Minafuro [et al.] // Technical Means of Information Protection: materials of XV Belarusian-Russian scientific and technical conference, Minsk, June 6, 2017. P. 28.

## A MODEL OF MULTI-KEY STEGANOGRAPHIC SYSTEM

P.P. Urbanovich, N.P. Shutko, A.M. Zapała

Recently, research to find new effective methods and tools of increasing the level of confidentiality of transmitted information, as well as protecting of content from unauthorized use are expanded and deepen. Main among these methods belongs to steganography. The steganographic system (steganosystem) – a set of tools and techniques that are used to form a secret channel of information transfer.

The processes of synthesis and analysis of steganographic systems are based on the use of models of such systems. The accuracy of the modeling of the steganographic systems and their investigation to obtain qualitative and quantitative estimates of the reliability of the use