THE SYSTEM OF MOBILE DEVICES PROTECTION AGAINST EAVESDROPPING

Project Manager. Andrii Biloshchytskyi, Doctor of Engineering Science, Full Professor

Project relevance. The vast majority of modern mobile devices (mobile phones) are practically not protected against information leaks by intercepting network traffic, as well as against unauthorized mobile microphone bugging by operator or spyware. It is possible to protect against eavesdropping only by removing power, but it is sometimes impossible. The situation is exacerbated by the fact that in some cases, cellular communication is a confidential information transmission channel. The known solutions are expensive and have a closed character, that does not allow to ensure in their reliability.

Project result. Hardware and software complex intended for additional protection of talks on cellular networks. It is assumed that on each mobile phone there will be installed the protected device for supplying/receiving the acoustic signal in the radio communication is encrypted/ decrypted form. At the same time, the speaker system built into the device to be blocked. The device is a wired / wireless headset with integrated hardware and software encryption module. The users can use their existing smartphones (disconnected from connection) or PC (laptop), which significantly reduce the cost of delivery.

Implementation area. The custom mobile communication devices used for transmission of important confidential data.

Academic achievements of the author. There are published more than 30 articles in the area of development of additional components for information security systems and defended a doctoral thesis.

Practical achievements of the author. There is developed the project of hardware and software.

Expected scientific value. There will be developed a methodology of creating additional protective equipment for custom mobile devices, allowing to increase the effectiveness of protection against eavesdropping with the help of blocking leakage channel, as well as through the introduction of additional cryptographic and stenographic means.

Expected practical efficiency. Providing public information system of protection against leakage, implemented by the interception of network traffic, as well as by listening to the microphone of the user device.

Development time. The first practical results (experimental hardware and software) will be available in a year.

Development cost. Salaries for workers, engaged in the process, the cost of purchasing parts.