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.

СИСТЕМА ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКИХ УСТРОЙСТВ СОТОВОЙ СВЯЗИ ОТ ПРОСЛУШИВАНИЯ

Керівник проекту. д.т.н., проф. Білощицький Андрій Олександрович

А**ктуальность проекта**. Подавляющее большинство современных пользовательских устройств сотовой связи (мобильных телефонов) практически не защищены от утечек информации за счет перехвата сетевого трафика, а также за счет несанкционированного прослушивания микрофона оператором мобильной связи или за счет программ-шпионов. Защититься от прослушивания можно лишь отключив питание, что иногда невозможно. Ситуация усугубляется тем, что в некоторых случаях сотовая связь является каналом передачи конфиденциальной информации. Известные решения дорогостоящие, имеют закрытый характер, что не позволяет удостовериться в их надежности.

Результат проекта. Аппаратно-программный комплекс, предназначенный для дополнительной защиты переговоров по сетям сотовой связи. Предполагается, что на каждом защищаемом пользовательском устройстве устанавливается девайс, предназначенный для подачи/приема акустического сигнала в радиоканал связи в зашифрованном/расшифрованном виде. При этом, акустическая система встроенная в устройство должна быть блокирована. Девайс представляет собой проводную/беспроводную границу интегрированную с аппаратно-программным модулем шифрования. В роли девайса может использоваться имеющийся у пользователя смартфон (отключенный от связи) или персональный компьютер (ноутбук), что существенно удешевит комплект поставки.

Предполагаемая сфера использования. Пользовательские устройства сотовой связи, предназначенные для передачи важной конфиденциальной информации.

Научные наработки авторов. В области разработки дополнительных компонент систем защиты информации опубликовано более 30 статей, защищена докторская диссертация..

Практические наработки авторов. Разработан проект аппаратно- программного комплекса.

Ожидаемая научная ценность. Будет разработана методология создания дополнительных средств защиты пользовательских устройств сотовой связи, позволяющая повысить эффективность защиты от прослушивания за счет блокирования каналов утечек, а также за счет внедрения дополнительных криптографических и стеганографичесих средств.

Ожидаемая практическая эффективность. Обеспечение общедоступной системы защиты информации от утечек, реализованных за счет перехвата сетевого трафика, а также путем прослушивания микрофона пользовательского устройства.

Срок разработки. Первые практические результаты (экспериментальное аппаратно-программное обеспечение) можно получить в течении года.

Расходы на разработку. Заработная плата исполнителей, расходы на покупку комплектующих.