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 гранитуру 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.