УДК 004.056

А.Н. ВАВИЧКИН, А.П. ДУРАКОВСКИЙ, Е.А. СИМАХИН
Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ И ВИБРАЦИОННЫМ КАНАЛАМ

Помещения, предназначенные для ведения конфиденциальных переговоров, содержащих сведения ограниченного доступа, подвергаются аттестационным испытаниям по требованиям безопасности информации. В докладе рассматриваются подходы к оценке защищенности речевой информации от утечки по акустическим и вибрационным каналам в соответствии новыми требованиями ФСТЭК России.

Работы по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, регламентируются приказом ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» и другими нормативными документами ФСТЭК России [1].

Наибольшую опасность непосредственного прослушивания речевой конфиденциальной информации, циркулирующей в помещениях для переговоров, представляют акустические и виброакустические каналы (воздуховоды, окна, трубопроводы, ограждающие конструкции).

Большинство коммерческих (и не только) компаний арендуют помещения в бизнес-центрах, где границей контролируемой зоны являются ограждающие конструкции помещения переговорной комнаты (защищаемое помещение), за которыми могут находиться конкуренты-злоумышленники. В данном случае невозможно обеспечить защиту речевой информации от прослушивания только пассивными методами, и требуется средства активной защиты помещений от утечки речевой информации. Для системы акустического и вибрационного зашумления применяют генераторы белого или розового шума в комплекте с набором акустических, электромагнитных и/или пьезоэлектрических вибропреобразователей [2].

Основной проблемой, от которой зависит эффективность защиты речевой информации, является выбор мест установки этих датчиков

(рис.1) [3], регулировка генератора по частотному диапазону, соответствующему ширине спектра речевого сигнала, по уровню шумов.

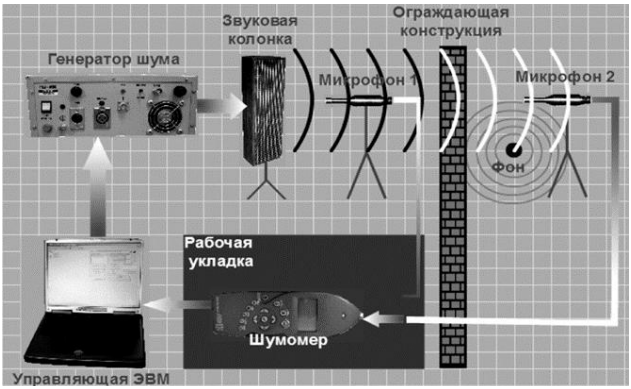

Рис. 1. Схема измерения уровня сигнала и фона в контрольной точке с использованием системы «Шёпот» [3]

Необходимо учитывать, что паразитные акустические шумы вносят дискомфорт, нарушают ведение нормальных переговоров в защищаемом помещении, и часто руководители просто отключают генераторы шума.

Не надо стремиться установить максимальное зашумление [4], минимальную защиту речевой информации можно обеспечить, когда уровень помехи приблизительно в три раза превышает уровень сигнала во всем частотном диапазоне или соотношение сигнал/помеха составляет минус 10 дБ. И этот результат должен повториться при многократных измерениях в контрольной точке.

Список литературы

1. Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.

2. Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации. Учебное пособие. – М.: НИЯУ МИФИ, 2015. – 152 с.

3. Бурлаков М.Е. Осипов М.Н. Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум: учебное пособие. – Самара: Издательство Самарского университета, 2021 – 96 с.

4. Дворянкин, Сергей В.; Антипенко, Антон О. Применение фазовых характеристик голосовых вокализмов в решении задач защиты речевой информации. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 21-33, апр. 2021. doi: http://dx.doi.org/10.26583/bit.2021.2.02.