АЛГОРИТМ КОНТРОЛЯ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТУТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Яцкевич М.С.

Дворникова Т.Н. – ст.преподаватель кафедры ИРТ, магистр технических наук

Информационная сфера играет все возрастающую роль в обеспечении безопасности всех сфер жизнедеятельности общества. Через эту сферу реализуется значительная часть угроз национальной безопасности государства.

Одними из основных источников угроз информационной безопасности являются деятельность иностранных разведывательных и специальных служб, преступных сообществ, организаций, групп, формирований и противозаконная деятельность отдельных лиц, направленная на сбор или хищение ценной информации, закрытой для доступа посторонних лиц.

Для предотвращения угроз информационной безопасности необходимо использовать алгоритмы контроля защищенности речевой информации от ее утечки по техническим каналам, так как с их помощью систематизируется проведение акустических измерений, обеспечивающих соответствующую защиту информации.

Разработка одного из алгоритмов определения защищенности речевой информации приведена в дипломной работе.

На рисунке 1 представлена схема размещения аппаратуры контроля при проведении акустических измерений для контрольной точки, не соответствующей возможному месту размещения ТСАРР.

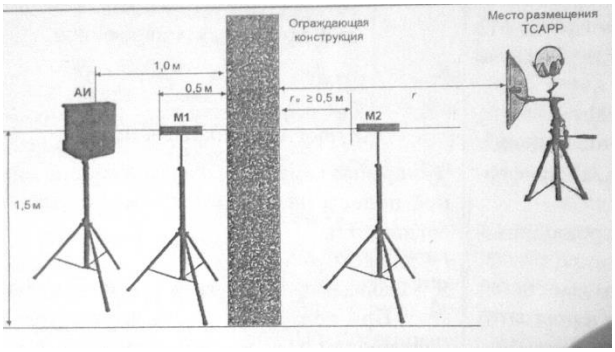

Рисунок 1 – Схема размещения аппаратуры контроля при проведении акустических измерений для контрольной точки, не соответствующей возможному месту размещения ТСАРР

АИ – акустический излучатель, М1 – измерительный микрофон, установленный в аттестуемом помещении, М2 – измерительный микрофон, установленный за пределами аттестуемого помещения.

Акустические измерения нужно проводить в период минимальной зашумлённости мест возможного нахождения средств акустической разведки. Во время проведения контроля измеряются среднеквадратические значения звукового давления.

Результатом проведения акустических измерений является словесная разборчивость, которая рассчитывается по формуле:

$$W_c = \begin{cases} 1{,}54 \cdot R^{0{,}25}[1 - exp(-11 \cdot R)], \text{если } R < 0{,}15; \\ 1 - exp\left(-\dfrac{11 \cdot R}{1 + 0{,}7 \cdot R}\right), \text{если } R \geq 0{,}15. \end{cases}$$

Словесная разборчивость речи W_c сравнивается с пороговым значением W_n.

Меры, принятые по защите выделенного помещения, считаются эффективны, если рассчитанное по итогам измерения значение словесной разборчивости речи W_c для каждой контрольной точки не превышает установленные нормы, то есть $W_c \leq W_n$.

В последнее время в связи с существенно возросшими объемами информации, передаваемой по техническим каналам, данный алгоритм контроля защищенности речевой информации является оптимальным, с точки зрения обеспечения защиты информации от утечки по техническим каналам.

Список использованных источников:

1. Железняк В.К. Защита информации от утечки по техническим каналам: учебное пособие / ГУАП. – СПб., 2006. – 188 с.: ил.

2. Хорев А.А. Техническая защита информации: учеб. Пособие для студентов. В 3 т. Т. 1. Технические каналы утечкиинформации. – М.: НПЦ «Аналитика», 2008. – 436 с.