УДК 621.396

ИССЛЕДОВАНИЕ ПРИНЦИПА РАБОТЫ ЗАКЛАДНЫХ РАДИОТЕХНИЧЕСКИХ УСТРОЙСТВ НЕСАНКЦИОНИРОВАННОГО СЪЕМА И ПЕРЕДАЧИ ИНФОРМАЦИИ

© Богдашкин А.Р., Жуков С.В.

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация

e-mail: bogdash999@gmail.com

За первое полугодие 2019 года аналитическим центром InfoWatch зарегистрировано 1276 случаев утечки конфиденциальной информации. Это на 22 % больше, чем за аналогичный период 2018 года (1039 утечек), 44,4 % из которых приходится именно на внешние атаки. Стоит сказать, что внешние атаки достаточно часто совершаются при помощи специальных закладных устройств, исследование принципов работы которых и является целью данного исследования [1].

Устройства передачи несанкционированных данных работают по принципу передатчика, который в постоянном режиме (пока не выйдет из строя аккумулятор закладного устройства) передает по радиоканалам связи ту или иную конфиденциальную информацию.

Устройства хранения и передачи несанкционированных данных работают по схожему принципу, но в отличие от предыдущего типа обладают встроенным устройством хранения информации (ПЗУ), который, в свою очередь, позволяет злоумышленнику передавать конфиденциальные данные в удобный временной период.

Зачастую нарушители безопасности маскируют сигнал, передаваемый закладным радиотехническим устройством несанкционированного съема и передачи данных, под всем известные частоты радиостанций.

Для того чтобы наиболее эффективно выполнять радиомониторинг выделенного помещения, необходимо делать это в течение некоторого времени (обычно 1–2 дня).

Алгоритм поиска сигнала выглядит следующим образом. Во-первых, нам необходимо считать значения диапазона частот с анализатора спектра. Используемый нами анализатор позволяет считать частоты от 0 Гц до 3 ГГц. На вход обнаружителя подается сигнал с выхода аналогово-цифрового преобразователя (АЦП) на промежуточной частоте (ПЧ). В качестве начальных условий принимаем, что сигнал является детерминированным на фоне узкополосного гауссовского шума с известным СКО ($\sigma = 1$), немодулированным информационным сообщением.

Затем нам необходимо сравнить сигнал с некоторыми эталонами. Для решения задачи поиска, обнаружения и идентификации сигнала может применяться процедура с комбинированной статистикой.

После этого, когда мы получим статистические данные вероятности присутствия того или иного сигнала на заданной частоте, мы можем с определенной долей вероятности сделать вывод о присутствии сигнала на заданной частоте (диапазоне частот).

Библиографический список

1. Сайт ГК InfoWatch. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года. 2019. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf.