В.А.ФЕДОРЕНКО[1], Д.Г.МУРАВИЦКИЙ[2]

ЗАЩИТА ДАННЫХ ПРИ РАБОТЕ В УСЛОВИЯХ РАДИОЭЛЕКТРОННОГО ПРОТИВОДЕЙСТВИЯ

[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, начальник цикла кафедры связи
[2]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, курсант

Современные радиоэлектронные системы передачи информации функционируют в условиях воздействия естественных и преднамеренных помех, способных привести к снижению достоверности приема, нарушению доступности и утечке передаваемых данных. В условиях радиоэлектронного противодействия защита информации должна обеспечивать не только сохранение ее содержания, но и устойчивость функционирования самого радиоканала. Согласно С. В. Козлову [1], радиоэлектронная защита информации представляет собой совокупность мер, способов и технических решений, направленных на предотвращение разрушения и несанкционированного извлечения информации. При этом для радиоэлектронных систем существенное значение имеют два взаимосвязанных свойства – помехоустойчивость и скрытность, совокупность которых характеризует помехозащищенность системы.

Одной из основных угроз является радиоэлектронная разведка, позволяющая обнаруживать радиоизлучение, определять его параметры и использовать полученную информацию для дальнейшего воздействия. Поэтому защита данных должна учитывать не только вероятность ошибки при приеме, но и возможность обнаружения самого факта работы радиоэлектронного средства. Другую группу угроз составляют активные помехи, воздействующие на полезный сигнал и изменяющие условия передачи информации. В результате возрастает вероятность ошибок и снижается достоверность приема.

Для повышения устойчивости радиоканала целесообразно использовать комплекс технических методов. В зависимости от различий между полезным сигналом и помехой применяются спектральные, временные, пространственные и пространственно-поляризационные методы обработки [1]. Их совместное использование позволяет выделять полезный сигнал на фоне мешающих воздействий. Дополнительным средством повышения скрытности и помехозащищенности могут выступать широкополосные сигналы. Увеличение базы сигнала обеспечивает снижение спектральной плотности его мощности и одновременно может повышать помехоустойчивость за счет расширения занимаемого спектра [1]. Структурная схема организации защищенной радиосвязи приведена на рисунке 1 [3].

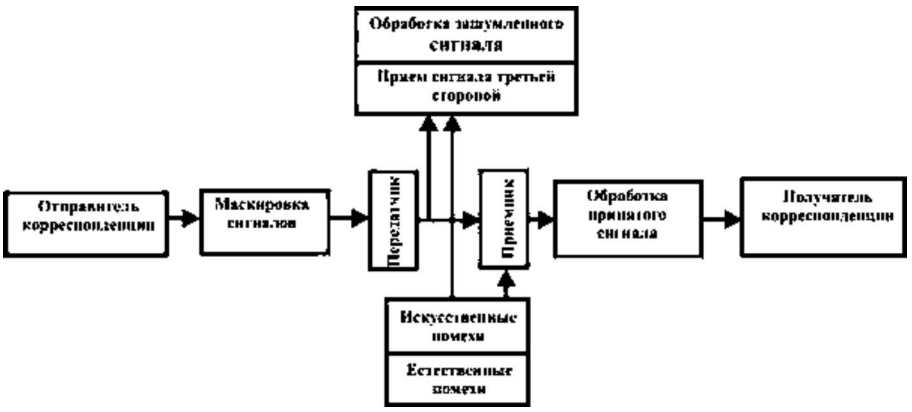


Рисунок 1 – Структурная схема организации защищенной радиосвязи

Представленная структура показывает, что защита данных должна обеспечиваться на нескольких этапах передачи. На передающей стороне применяются кодирование и криптографическое преобразование информации, а при необходимости – дополнительные меры маскировки. На приемной стороне выполняются выделение полезного сигнала, декодирование и расшифрование.

Важную роль играет помехоустойчивое кодирование. Введение избыточности в передаваемую последовательность позволяет обнаруживать и исправлять часть ошибок, возникающих под воздействием помех. Однако кодирование решает преимущественно задачу повышения достоверности передачи и не обеспечивает конфиденциальность содержания сообщения. Поэтому для комплексной защиты данных оно должно дополняться криптографическими методами [2], обеспечивающими защиту информации при ее возможном перехвате.

Для рассмотрения количественных характеристик обнаружения радиосигналов обратимся к результатам научного исследования С. А. Ковтуна, С. В. Ковальчука и П. П. Топольницкого «Статистические характеристики энергетически скрытого фазоманипулированного сигнала» [4]. В работе рассматриваются статистические характеристики кодофазоманипулированного сигнала на фоне белого шума при использовании некогерентного автокорреляционного приемника с квадратурной обработкой. Авторы исследуют возможность обнаружения энергетически скрытого сигнала при низком отношении сигнал/шум. При отсутствии полезного сигнала распределение выходного эффекта соответствует закону Рэлея, а при его наличии – закону Рэлея–Райса [4]. Полученные результаты позволяют оценить возможности обнаружения слабых радиосигналов, что имеет значение для обеспечения скрытности связи в условиях радиоэлектронного противодействия.

Одним из параметров, рассматриваемых авторами, является время накопления входной смеси. Авторы показывают, что его изменение оказывает существенное влияние на минимальное отношение сигнал/шум, при котором возможно обнаружение сигнала. Для удобства анализа численные результаты, приведенные авторами исследования, представлены в таблице 1 [4].

Таблица 1 – Результаты исследования обнаружения энергетически скрытого фазоманипулированного сигнала

Время накопления T, с	Вероятность ложной тревоги P_F	Вероятность правильного обнаружения P_D	Входное отношение сигнал/шум, дБ
10^{-3}	10^{-3}	0,9	−22,6
10^{-3}	10^{-6}	0,9	−21,4
10^{-1}	10^{-3}	0,9	−32,6
10^{-1}	10^{-6}	0,9	−31,4

Из таблицы видно, что увеличение времени накопления с 10^{-3} до 10^{-1} с позволяет обнаруживать фазоманипулированный сигнал при существенно меньшем отношении сигнал/шум. При вероятности ложной тревоги $P_F = 10^{-3}$ требуемое входное отношение сигнал/шум изменяется с −22,6 до −32,6 дБ. Таким образом, при увеличении времени накопления на два порядка обнаружение сигнала с вероятностью правильного обнаружения P_D = 0,9 становится возможным при отношении сигнал/шум на 10 дБ ниже.

Аналогичная зависимость наблюдается при вероятности ложной тревоги $P_F = 10^{-6}$: требуемое отношение сигнал/шум изменяется с −21,4 до −31,4 дБ. Следовательно, увеличение времени накопления существенно повышает возможности обнаружения слабого радиоизлучения. Это особенно важно при рассмотрении радиоэлектронной разведки, поскольку даже сигнал с низким энергетическим уровнем может быть обнаружен при достаточно продолжительном наблюдении.

Рассмотренные результаты имеют непосредственное значение для защиты данных в условиях радиоэлектронного противодействия. Они показывают, что даже при низком энергетическом уровне радиосигнал может быть обнаружен при достаточно продолжительном наблюдении. Поэтому при организации защищенной радиосвязи необходимо учитывать не только достоверность передачи, но и возможность обнаружения радиоизлучения средствами радиоэлектронной разведки.

Одним из направлений повышения скрытности является применение фазоманипулированных и широкополосных сигналов, позволяющих снизить энергетическую заметность радиопередачи. При этом их применение должно сочетаться с методами обработки, обеспечивающими требуемую достоверность приема при воздействии помех. В зависимости от характера помеховой обстановки могут использоваться спектральные, временные и пространственные методы обработки, а также помехоустойчивое кодирование [1].

При этом технические средства защиты радиоканала должны дополняться криптографическими методами. Даже при снижении вероятности обнаружения радиопередачи полностью исключить возможность перехвата сигнала невозможно. Криптографическое преобразование позволяет обеспечить конфиденциальность содержания информации в случае получения противником передаваемого сигнала [2]. Таким образом, скрытность и помехоустойчивость направлены преимущественно на защиту процесса передачи, тогда как криптографические методы обеспечивают защиту самого содержания информации.

Рассмотренное научное исследование показывает, что при оценке защищенности радиоэлектронных систем необходимо учитывать возможность обнаружения радиоизлучения средствами радиоэлектронной разведки. Представленные авторами результаты демонстрируют зависимость возможностей обнаружения слабого фазоманипулированного сигнала от времени накопления и отношения сигнал/шум. Это подтверждает необходимость комплексного подхода к защите данных, включающего повышение помехоустойчивости, снижение энергетической заметности радиопередачи и криптографическую защиту информации.

Таким образом, ознакомление с результатами существующих научных исследований позволяет определить перспективные направления защиты данных при работе в условиях радиоэлектронного противодействия. Рассмотренный пример показывает, что обеспечение безопасности радиоканала не сводится только к повышению достоверности передачи: необходимо одновременно учитывать устойчивость к помехам, вероятность обнаружения радиоизлучения и возможность перехвата передаваемой информации. Комплексное применение соответствующих технических и криптографических методов позволяет повысить устойчивость радиоэлектронных систем к различным видам воздействия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Козлов, С. В. Методы и средства радиоэлектронной защиты : учеб. пособие / С. В. Козлов. – Минск : БГУИР, 2019. – 188 с.

2. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М. : Гелиос АРВ, 2002. – 480 с.

3. Федулина, И. Н. Защита информации в радиоэлектронных системах : конспект лекций / И. Н. Федулина. – Алматы : АУЭС, 2011. – 73 с.

4. Ковтун, С. А. Статистические характеристики энергетически скрытого фазоманипулированного сигнала / С. А. Ковтун, С. В. Ковальчук, П. П. Топольницкий // Проблемы создания, испытания, применения и эксплуатации сложных информационных систем. – 2019. – Вып. 16. – С. 108–114. – DOI: 10.46972/2076-1546.2019.16.10.