ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА «ЭРА», 2023, том 4, № 4, с. 379–382

ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

УДК 004.056.53

УГРОЗЫ БЕСПРОВОДНЫМ КАНАЛАМ ПЕРЕДАЧИ ИНФОРМАЦИИ РАЗЛИЧНЫХ СРЕДСТВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ И СПОСОБЫ ИХ НЕЙТРАЛИЗАЦИИ

© 2023 г. М. И. Заховаев[1], Е. О. Шмаков[1], В. А. Щербаков[1], А. А. Тырышкин[1,*], И. В. Вакуленко[1]

[1]*Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, Краснодар, Россия*

******E-mail: taa17071987@rambler.ru*

Поступила в редакцию 20.11.2023 г.
После доработки 20.11.2023 г.
Принята к публикации 26.11.2023 г.

Исследованы возможные угрозы беспроводным каналам передачи информации различных средств специального назначения, а также существующие криптографические и некриптографические методы и средства их нейтрализации. Ввиду физических особенностей радиоканала и наибольшей подверженности его к внешним угрозам сделано заключение об особой важности применения некриптографических средств защиты информации, обеспечивающих помехоустойчивость и скрытность. На основе проведенного анализа сформированы требования безопасности, предъявляемые к беспроводным каналам связи.

DOI: 10.56304/S2782375X23040174

ВВЕДЕНИЕ

Процесс организации системы защиты данных как в каналах связи, так и в других информационных системах (**ИС**) в целом включает в себя следующие этапы:

– анализ возможных угроз;

– планирование комплекса мер защиты;

– реализация комплекса мер защиты;

– сопровождение применяемых мер защиты.

Наиболее важным этапом обеспечения безопасности ИС является этап анализа возможных угроз, он необходим для фиксации состояния ИС (конфигурации аппаратных и программных средств, технологии обработки информации) и определения учитываемых воздействий на компоненты системы [1]. В зависимости от физической среды передачи комплексы методов защиты информации имеют свои особенности.

В данной работе рассмотрим угрозы, которые возникают при передаче информации по беспроводным каналам связи, а также существующие методы и средства их нейтрализации. На основе проведенного анализа сформированы требования безопасности, предъявляемые к беспроводным каналам связи.

УГРОЗЫ БЕСПРОВОДНЫМ КАНАЛАМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Для организации каналов связи между компонентами, сегментами, пунктами управления систем специального назначения в качестве среды передачи применяются медные линии, оптоволокно и радиоканал. Требования к защищенности информации, передаваемой по радиоканалам, прежде всего определяются физическими особенностями функционирования каналов связи информационных систем.

При использовании для передачи данных радиоканала значительно увеличивается вероятность обнаружения, перехвата и модификации передаваемых данных. В отличие от проводных каналов связи сетевой трафик в беспроводной сети сильнее подвержен прослушиванию и перехвату радиотехническими средствами злоумышленника. Осуществить данные действия возможно использованием всего лишь пассивного приемника, настроенного на частоту передающего устройства. При этом факт перехвата в большинстве случаев установить невозможно.

Для определения методов и средств защиты информации для ее передачи по беспроводному каналу связи необходимо провести анализ возможных угроз.

Существующие угрозы безопасности радиолинии можно условно разделить на пассивные и ак-

тивные. При пассивном вторжении нарушитель только просматривает и анализирует информационный поток, не оказывая никакого воздействия. При активных угрозах злоумышленник оказывает непосредственное воздействие на радиолинии или передаваемую по ней информацию. Все возможные угрозы воздействия противника на радиолинии при их реализации позволяют ему нарушить конфиденциальность, целостность или доступность передаваемой по радиолинии информации [2]. Противник может реализовать угрозу безопасности на всех логических уровнях обработки информации в ИС. Для обоснованного применения механизмов защиты необходимо подробно рассмотреть возможные виды угроз. Можно выделить четыре основные угрозы беспроводным каналам передачи информации:

– просмотр информации или радиоэлектронная разведка. Данная угроза является пассивной и направлена на установление (раскрытие) самого факта передачи данных. В этом случае нарушитель только наблюдает за прохождением информации по каналу связи, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации;

– перехват информации или радиоэлектронный перехват. Такая угроза является следствием радиоэлектронной разведки и также относится к пассивным. Она направлена на перехват и получение содержимого передаваемых данных, вскрытие их семантической составляющей в основном путем применения средств криптоанализа;

– подмена. Такой вид угроз относится к ряду активных и направлен на нарушение целостности информации, передаваемой по каналу связи, путем искажения или внедрения ложных данных в пункты управления;

– подавление. Данный вид угрозы направлен на срыв или ухудшение качества информационного обмена, как правило, путем создания агрессивной среды для канала связи, что достигается при воздействии помех. Создание преднамеренных помех является одним из основных способов ведения радиоэлектронной борьбы.

Результатами первой угрозы являются обнаружение факта информационного обмена, определение радиочастотных параметров сигнала (несущей частоты, ширины полосы частот, источника передачи) и анализ обнаруженного трафика (определение идентификатора, длины сообщения, частоты обмена, анализ признаков применения средств криптографической защиты информации к передаваемым данным и просмотр содержимого сообщений в случае, если данные не зашифрованы).

Следствием перехвата является нарушение конфиденциальности информации, компрометация ключевой документации, перехват и вскрытие зашифрованных данных в результате криптоанализа, в частности раскрытие содержания телеметрической информации, командно-программной информации, специальной информации ограниченного распространения (данные разведки, команды управления).

Угроза подмены заключается в возможности перехвата и целенаправленного искажения существующих или навязывания ложных данных: телеметрической, навигационной, командно-программной и другой специальной информации. В результате чего адресат может получать информацию от злоумышленника, считая, что информация идет от доверенного источника. Таким образом противник может перехватить управление ИС.

Радиоэлектронное подавление радиосигнала за счет направленного воздействия помех большой мощности приводит к ошибкам на входе приемника или полному подавлению радиоканала и срыву сеанса обмена, а в наихудшем случае – к выведению из строя технических средств связи.

МЕТОДЫ И СРЕДСТВА НЕЙТРАЛИЗАЦИИ УГРОЗ

Анализ приведенных угроз позволяет выделить следующие средства их нейтрализации:

– криптографические;

– не криптографические.

Криптографические методы основаны на применении программных и аппаратных средств, реализующих специальные алгоритмы шифрования, кодирования и иного преобразования информации, в результате которого ее содержание становится недоступным при передаче по каналам связи, а также при обработке и хранении данных. Существуют следующие основные средства криптографической защиты:

– средства шифрования – аппаратные, программные средства, осуществляющие криптографическое преобразование данных с использованием симметричного или асимметричного шифрования для передачи данных по каналу связи;

– средства имитозащиты – аппаратные, программные средства, осуществляющие криптографическое преобразование данных и предназначенные для защиты целостности информации;

– средства электронной цифровой подписи (**ЭЦП**) – аппаратные и программные средства, обеспечивающие на основе криптографических преобразований создание ЭЦП, подтверждение подлинности ЭЦП, создание закрытых и открытых ключей для шифрования и расшифрования ЭЦП. Цифровая подпись позволяет подтвердить целостность информации и подлинность источника.

Не криптографические методы защиты информации связаны с физическими и организационными особенностями передачи данных по радиоканалу. Основной задачей не криптографических средств защиты является решение проблем помехозащищенности информационной системы.

Помехозащищенностью называют способность радиоэлектронных средств функционировать с заданным качеством в условиях ведения противником радиоразведки и создания им преднамеренных помех [3].

Решение этой проблемы заключается в повышении скрытности и помехоустойчивости ИС и канала связи.

Меры обеспечения помехоустойчивости направлены на создание условий, при которых достоверность извлекаемой информации не должна уменьшаться ниже допустимого уровня. Учитывая, что помехи могут находиться в широком диапазоне частот, необходимо использовать эффективные методы борьбы с помехами.

Воздействию помех, как правило, предшествует этап радиоэлектронной разведки и, как следствие, обнаружение факта передачи и измерение радиочастотных параметров сигнала. Потому решение проблемы помехоустойчивости достигается методами обеспечения скрытности функционирования радиосистем.

Методы повышения скрытности сводятся прежде всего к выбору такого вида излучаемого сигнала, который затрудняет обнаружение этого сигнала и измерение его основных параметров с целью создания преднамеренных помех [4].

Скрытность информации достигается методами энергетического, временного, частотного или пространственного скрытия, а также проведением организационных мероприятий.

Энергетическое скрытие осуществляется путем уменьшения соотношения сигнал/помеха за счет снижения мощности излучаемого сигнала или применения шумоподобных сигналов. Шумоподобными называют такие сигналы, у которых произведение ширины спектра (F) на длительность (T) много больше единицы. В системах связи с шумоподобными сигналами ширина спектра F всегда много больше ширины спектра передаваемого сообщения [5]. Временная скрытность достигается за счет временного распределения передачи данных и уменьшения длительности излучаемого сигнала. Частотный метод сводится к перестройке рабочих частот – несущей частоты повторения импульсов. В частотном скрытии наиболее эффективным является метод псевдослучайной перестройки рабочей частоты, заключающийся в постоянной смене несущей частоты в соответствии с псевдослучайной последовательностью чисел, известной как отправителю, так и получателю. Данный метод относят к методам расширения спектра. Пространственная скрытность обеспечивается сужением диаграммы направленности антенн и уменьшением уровня их боковых лепестков, а также разнесением передающей и приемной позиций.

Кроме перечисленных существует множество других структурно-алгоритмических и иных технических методов повышения помехоустойчивости ИС. К ним относятся: применение помехоустойчивого кодирования, адаптивное кодирование, скремблирование, адаптивная модуляция, использование сигналов с расширенным спектром, увеличение мощности и коэффициента усиления, применение методов селекции и компенсации помех.

На канальном уровне эффективной мерой для обеспечения помехоустойчивости информации являются методы канального помехоустойчивого кодирования. Использование данного кодирования ведет к увеличению избыточности информации.

Для исключения помеховой составляющей из принимаемого сигнала путем анализа возможных отличий его параметров применяются методы частотной, фазовой, временной, амплитудной и пространственной селекции.

Адаптивная модуляция заключается в изменении индекса модуляции либо в изменении типа модуляции сигнала. Увеличение порядка модуляции позволяет повысить скорость передачи информации, но при этом повышает вероятность ошибки.

Еще одним не криптографическим методом защиты информации является дезинформация. Она основана на передаче ложных сигналов, что является эффективным способом борьбы с радиоэлектронной разведкой злоумышленника.

На основании изложенного можно сделать выводы о том, что криптографические средства защиты направлены на обеспечение конфиденциальности и целостности передаваемых данных, что обеспечивает защиту информации от угроз перехвата и подмены. Для защиты информации от просмотра применяются средства скрытия информации, которые, в свою очередь, решают проблему помехозащищенности сети. Для противодействия случайным помехам применяются методы избыточного кодирования данных; а для защиты от радиоэлектронного подавления применяются методы скрытия и другие технические средства, обеспечивающие помехоустойчивость ИС. Для реализации эффективной защиты информации в радиоканале требуется применять данные технические средства комплексно, однако совместное применение указанных методов приводит к задержкам в процессе передачи данных или увеличивает вероятность возникновения ошибки.

ОБЩИЕ ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К БЕСПРОВОДНЫМ КАНАЛАМ СВЯЗИ РАЗЛИЧНЫХ СРЕДСТВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

На основании проведенного анализа возможных угроз в беспроводных каналах связи и способов их нейтрализации, а также в соответствии с нормативными документами РФ (ГОСТ, ОТТ, приказов Минобороны России, ФСБ, ФСТЭК и др.) можно сформулировать следующие требования к радиоканалу:

– создана защита от нарушения конфиденциальности и изменения информации, передаваемой по радиоканалу;

– обеспечена целостность данных при передаче по радиоканалу;

– реализованы средства, обеспечивающие невозможность раскрытия внутренней структуры сети при перехвате сообщений;

– реализованы средства, обеспечивающие помехозащищенность и помехоустойчивость передаваемых данных;

– использована надежная система аутентификации и обмена ключей;

– использован криптографически стойкий алгоритм защиты информации;

– обеспечена возможность работы ИС в сложной электромагнитной обстановке, при наличии естественных и преднамеренных помех, а также в условиях многолучевого распространения сигналов;

– обеспечено наличие режимов адаптации по излучаемой мощности, пропускной способности и частоте излучения в зависимости от помеховой обстановки и дальности управления;

– реализована максимально скрытная радиосвязь и обеспечена разведзащищенность канала;

– обеспечена защита ИС от опасных программно-технических воздействий;

– обеспечена защита ИС от несанкционированного доступа [6–8].

ЗАКЛЮЧЕНИЕ

Таким образом, радиоканал является наиболее уязвимой средой передачи ввиду физических особенностей распространения радиоволн. При этом радиоканал подвергается систематическим атакам со стороны противника с применением современных технических средств радиоразведки, радиоперехвата и радиоподавления.

Несмотря на неопределенность понятия защищенность, особенностью радиолинии является то, что как бы не были хороши криптографические методы защиты информации на программном уровне, изменение значения сигнала при сложении его с помеховым сигналом в приемном тракте приведет к искажению информации и ошибке на входе приемника. Поэтому при планировании и реализации комплекса мер защиты информации при передаче ее по радиоканалу особое внимание необходимо акцентировать на средствах обеспечения помехоустойчивости и скрытности.

СПИСОК ЛИТЕРАТУРЫ

1. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / Под ред. Шаньгина В.Ф. 2-е изд., перераб. и доп. М.: Радио и связь, 2001. 376 с.
2. *Антохин Е.А., Панасенко Н.Н., Чернова А.Д.* // Робототехника и техническая кибернетика. 2017. № 4 (17). С. 10.
3. *Ряховский Е.П.* Шумоподобные сигналы в каналах управления космическими аппаратами. Часть 2. Принципы применения: учебное пособие. СПб.: ВКА им. А.Ф. Можайского, 2014. 223 с.
4. *Сосулин Ю.Г.* Теоретические основы радиолокации и радионавигации: Учеб. пособие для вузов. М.: Радио и связь, 1992. 304 с.
5. *Варакин Л.Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь. 1985, 384 с.
6. ГОСТ РВ 51987-02 “Типовые требования и показатели качества функционирования информационных систем”.
7. ГОСТ В 25232-82 “Совместимость радиоэлектронных средств электромагнитная. Порядок обеспечения электромагнитной совместимости”.
8. ГОСТ РВ 20.39.302-98. “Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Требования к программам обеспечения надежности и стойкости к воздействию ионизирующих и электромагнитных излучений”.