ПРЕДИСЛОВИЕ

Учебное пособие представляет собой результат учебно-методической, научно-исследовательской и практической деятельности авторского коллектива специалистов в области защиты информации. В предлагаемых читателю материалах систематизирован опыт авторов в области построения и защиты телекоммуникационных систем.

Целью данного издания является представление системных знаний по основам физических процессов, связанных с защитой информации в мобильных системах связи в условиях угроз прослушивания, модификации и подмены передаваемой информации. В работе рассмотрены особенности построения и функционирования современных систем мобильной связи, теоретические основы и практика реализации методов защиты информации в них.

Содержание учебного пособия построено на открытых материалах отечественных и зарубежных литературных источников, а также авторских разработок в области защиты информации в мобильных системах связи.

Учебное пособие «Защита информации в системах мобильной связи» предназначено для использования в учебном процессе для образовательной системы высшего профессионального образования по специальности 075600 – Информационная безопасность телекоммуникационных систем.

Кроме того, данное издание может быть полезно при реализации послевузовского повышения квалификации специалистов в области проектирования и эксплуатации защищенных телекоммуникационных систем.

ВВЕДЕНИЕ

Возросшие требования к оперативности информационных процессов в различных областях деятельности современного общества, а также расширение возможностей сетевого построения информационных систем и внедрение методов распределенной обработки данных за счет реализации теледоступа к вычислительным средствам привели к появлению и развитию систем мобильной связи (СМС), представляющих собой результат интеграции систем обработки информации и систем ее обмена. Наиболее широкое применение такие системы нашли в так называемых сферах критических приложений, к которым относится деятельность институтов государственной власти, правоохранительных органов, финансовых структур, деятельность в областях военно-промышленного ком-

плекса, энергетики, транспорта, а также в областях, оказывающих существенное влияние на экологию. Несмотря на очевидную разнородность сфер критических приложений, их объединяет одно очень важное обстоятельство – значительный ущерб от нарушения безопасности деятельности, в том числе и информационной, в этих сферах. Вытекающая из этого значительная ценность хранимых и обрабатываемых данных в СМС сфер критических приложений обусловила разработку и совершенствование методов и средств противоправного доступа и манипулирования информацией в этих системах.

Одним из основных каналов утечки информации в системах мобильной связи являются каналы радиосвязи, обеспечивающие привязку мобильных абонентов к базовым станциям, обеспечивающим дальнейшую передачу информации по каналам многоканальных систем связи общего пользования либо ведомственной принадлежности. Основным недостатком каналов радиосвязи является доступность передаваемых сигналов к перехвату с целью прочтения, разрушению и модификации передаваемой информации.

Названная особенность каналов связи обусловливает необходимость применения в интересах обеспечения информационной безопасности специальных методов обработки и передачи информации. Известно большое количество таких методов, исследованных в большом числе работ отечественных и зарубежных авторов. В этих трудах разработаны основные теоретические положения обеспечения защиты информации в каналах радиосвязи, методологические и научно-теоретические основы построения защищенных систем связи, модели источников и каналов утечки информации, методики оценки защищенности информации при ее передаче, хранении и обработке. Вместе с тем к настоящему времени отсутствует системное изложение теоретических положений и практических особенностей реализации методов защиты информации в системах мобильной связи.

Целью данного учебного пособия является анализ методов защиты информации и особенностей их реализации в системах мобильной связи на примере СМС массового применения стандартов GSM и IS-95. Каналы СМС стандартов GSM и IS-95 широко используются в сфере критических приложений для передачи информации конфиденциального характера (с грифом, не превышающим «Для служебного пользования»), не содержащей сведений, составляющих государственную тайну (с грифом «Секретно» и выше). Это и определяет интерес со стороны злоумышленников, подвергающих каналы СМС информационным атакам с целью копирования, прочтения, разрушения или модификации информации.

В учебном пособии системно изложены особенности построения защищенных систем мобильной связи, а также основные направления решения проблемы обеспечения их информационной безопасности. В пособии представлены:

- понятийный аппарат, используемый при описании систем мобильной связи;
- история появления и развития систем мобильной связи;
- особенности построения и функционирования систем мобильной связи;
- особенности применения принципов частотно-территориального планирования в интересах обеспечения защиты информации в мобильных системах связи;
- угрозы информационной безопасности СМС как телекоммуникационных систем;
- основы защиты информации в телекоммуникационных системах;
- особенности реализации мер защиты информации в системах мобильной связи стандартов GSM и IS-95;
- особенности защиты информации в перспективных системах мобильной связи.

Новизна данного учебного пособия состоит в том, что в нем на основе анализа существующих теоретических подходов к защите информации в СМС осуществлено системное изложение принципов обеспечения их информационной безопасности.

Представленный в учебном пособии материал позволит специалистам значительно повысить обоснованность управленческих решений по организации деятельности в сферах критических приложений, выработать практические рекомендации по внедрению новых информационных технологий, исследовать пути построения защищенных систем мобильной связи. Кроме того, учебное пособие может быть полезно специалистам по информационной безопасности, в круг задач которых входит выявление и пресечение преступных посягательств на информацию в такой специфичной области, как системы мобильной связи.