УДК 621.377

А.С. Корсунский

О НЕКОТОРЫХ ПРОБЛЕМАХ ПРОТИВОБОРСТВА В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Корсунский Андрей Сергеевич, *кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру Военной академии связи им. С.М. Буденного. Главный специалист ФНПЦ ОАО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации, а также передачи информации по беспроводным каналам связи информационно-телекоммуникационных систем. [e-mail: aksspb@mail.ru].*

Аннотация

В данной статье исследуются вопросы противоборства в современных информационных системах. Рассмотрены современные методы криптографической и стеганографической защиты информации.

Ключевые слова: информационное противоборство, криптография, стеганография, аутентификация.

Введение

Рассмотрим некоторые проблемы информационного противоборства в системах и сетях, связанные с развитием и использованием современных методов криптографической и стеганографической защиты информации.

В процессе информационного противоборства между легальными корреспондентами (пользователями информации) и злоумышленниками противостоящие стороны добиваются, в частности, определенных целей.

Целями законного пользователя или владельца защищаемой информации могут быть:

– сохранение в тайне сообщений и факт их передачи или хранения;

– обеспечение подлинности сообщений;

– исключение неавторизованного использования информации.

Возможные цели злоумышленника:

– чтение защищаемой информации и отслеживание информационного трафика;

– искажение, блокирование передаваемых сообщений, навязывание ложной информации;

– несанкционированное использование не принадлежащей ему информации.

Ряд задач защиты информации традиционно решается путем использования криптографических систем [1]. В соответствии с выполняемыми задачами среди криптографических систем можно выделить два основных класса: криптосистемы, обеспечивающие секретность (конфиденциальность) информации, и крип-

тосистемы, обеспечивающие подлинность (аутентичность) информации. Такое разделение обусловлено тем, что задача защиты секретности информации (сохранения ее в тайне) принципиально отличается от задачи защиты подлинности информации (исключение подделки) и поэтому должна решаться другими криптографическими методами.

Криптосистемы аутентификации информации предназначены для контроля подлинности информации, но в ряде случаев они способны эффективно обеспечить контроль ее целостности при различных деструктивных воздействиях.

Проблемы противоборства в информационных системах

Рассмотрим некоторые проблемы сохранения в тайне передаваемых сообщений и факта их передачи. В рамках криптографических систем к настоящему времени разработаны системы шифрования информации, криптостойкость которых вполне достаточна для большинства их применений. Совершенствование современных шифров происходит в основном по линии повышения скорости криптографических преобразований при использовании программных или аппаратных методов их реализации и достижении сопряжения с современными технологиями обработки информации. Однако системы шифрования не способны скрыть от противника факт защищенной передачи информации. Криптограммы произвольных систем шифрования неотличимы только от безызбыточного бернуллиевского источника сообщений. Большинство передаваемых сообщений описывается иными законами распределения и имеет существенную избыточность, поэтому шифрованная передача телефонных, телеграфных, факсимильных и видеосообщений и большей части передаваемых данных легко выявляется на фоне открытой передачи сообщений этих же источников.

Кроме криптографических методов сохранения информации в тайне, интенсивно разрабатываются стеганографические методы защиты ее секретности. Под стеганографией понимается область методов защиты информации, в которой скрывается не только содержание передаваемых сообщений, но и сам факт их передачи. Заметим, что в криптографии не ставится задача утаить от противника факт передачи защищаемой информации и, как правило, в рамках криптографических систем решение этой задачи невозможно. В своем развитии стеганография от примитивных методов сокрытия сообщений, таких как использование для секретной почтовой переписки «невидимых» чернил, перешла в качественно новый этап своего развития, называемый электронной стеганографией. Подобно тому как в конце сороковых годов двадцатого столетия криптография стала наукой, в последние годы электронная стеганография приобретает черты самостоятельной науки о защите информации. Бурному взлету стеганографии способствовало то, что она вобрала в себя достижения современной криптографии, теории информации, цифровой обработки сигналов, теории и практики передачи сообщений.

Рассмотрим обобщенную модель стеганографической системы передачи сообщений [2]. Скрытое сообщение прячется в открытой информации, называемой контейнером. Отправитель и получатель скрытых сообщений используют секретный ключ, доставляемый им по защищенным от противника каналам. Встраивание

в контейнер скрытого сообщения под управлением секретного ключа выполняется в кодере, с выхода которого стегограмма передается по незащищенному каналу связи. В этом канале противник, осведомленный в соответствии с принципом Керкгоффа с основами построения стегосистемы и статистическими характеристиками скрытых сообщений и контейнеров, пытается установить факт передачи секретных сообщений и прочитать их. Контейнеры в стегосистемах могут быть предопределенными (фиксированными вне зависимости от конкретных скрытых сообщений) или формируемыми под конкретные скрытые соообщения. Также возможны поточные контейнеры, например, представляющие собой осмысленные открытые сообщения, которые необходимо с требуемым качеством доставить получателю контейнерных сообщений. Аналогично известным оценкам стойкости криптосистем определены оценки стойкости стегосистем. Например, с позиций теории информации определено понятие безусловной стойкости стегосистем. Существуют также и классификации типов атак противника на стегосистемы, например атака противника со знанием исходного вида контейнера, атака противника на стегосистему с выбранным скрытым сообщением и т. д.

Скрытый канал передачи информации может быть организован как легальным пользователем открытого канала, так и злоумышленником, способным скрытно передавать свою информацию по чужой системе связи, а также незаконным пользователем, бесплатно использующим чужой информационный ресурс, ухудшая при этом качество связи законного пользователя.

К настоящему моменту предложено большое количество конструктивных способов сокрытия сообщений, поступающих из различных источников, в контейнерах: сокрытие электронного изображения в изображении, данных в изображении, телеграфных сообщений в цифровом речевом сигнале. Однако известные зарубежные и отечественные стеганографические средства защиты информации ориентированы преимущественно на использование в сетях, подобных Интернету, и в основном предназначены для сокрытия сообщений в видеоданных большого объема. Не менее актуальной является задача передачи скрытых речевых сообщений в открытых речевых сообщениях, передаваемых по каналам, доступным злоумышленникам. Например, скрытное ведение телефонных переговоров под прикрытием открытых речевых сообщений в сетях открытой телефонной связи, радио и проводной.

Для практической реализации подобных методов скрытой связи необходимо решить ряд характерных для существующих стеганографических методов защиты информации проблем:

1. Малый объем скрытно передаваемой информации по сравнению с объемом контейнера.
2. Низкая устойчивость к воздействию ошибок передачи известных каналов скрытой передачи информации.
3. Необходимость подбора контейнера для вложения скрытого сообщения.
4. Отсутствие методов сокрытия информации, применяемых в режиме реального времени.

Однако существующие строгие оценки теоретически достижимой скорости

канала скрытой передачи информации позволяют полагать, что задачи скрытой передачи сообщений объема, сопоставимого с объемом контейнера, в режиме, близком к реальному времени, по каналам связи с помехами имеют теоретическое и практическое решение.

Рассмотрим также некоторые проблемы обеспечения подлинности передаваемых сообщений [3–7]. Класс методов криптографической защиты информации от подделки может быть разделен в зависимости от решаемой задачи на методы аутентификации информации (сообщений) и методы аутентификации источников или объектов информации (корреспондентов, пользователей, сетей, систем и т. п.). Рассмотрим случай, когда требуется проверить подлинность информации, передаваемой от отправителя ее получателю, безусловно, доверяющих друг другу: законные корреспонденты или пользователи не могут обманывать друг друга, и только внешний нарушитель может искажать информацию. Криптосистемы аутентификации сообщений при таких условиях используют формирование и проверку имитовставок сообщений. Имитовставка – это отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты [8]. Получатель зашифрованного сообщения и его имитовставки, имея такой же секретный ключ, способен из расшифрованного сообщения и ключа заново сформировать имитовставку и при ее совпадении с полученной имитовставкой из канала связи убедиться в отсутствии искажений полученного сообщения. В случае, когда требуется проверить подлинность информации, передаваемой от отправителя к получателю, не доверяющим друг другу, криптосистемы аутентификации на основе имитовставок неэффективны. Так как получатель и отправитель сообщений обладают одинаковой ключевой информацией, они относительно друг друга потенциально могут осуществить следующие обманные действия (атаки):

– ренегатство − отправитель заявляет, что он не посылал сообщение получателю, хотя на самом деле посылал;

– переделку − получатель искажает сообщение, полученное им от отправителя, и утверждает, что автором искаженного сообщения является отправитель;

– подмену – отправитель ничего не передает, а получатель формирует ложное сообщение и утверждает, что получил его от отправителя.

Подлинность информации в условиях взаимного недоверия сторон может быть обеспечена путем использования цифровой подписи сообщения, формируемой отправителем и проверяемой получателем сообщений. Невозможность выполнения каких-либо действий отправителя за получателя и получателя за отправителя при использовании цифровой подписи сообщения обусловлена тем, что они для выполнения криптографических преобразований, таких как формирование и проверка цифровой подписи сообщения, используют различную ключевую информацию.

Основным недостатком перечисленных способов аутентификации сообщений является низкая устойчивость аутентифицированных сообщений к ошибкам передачи. Для признания полученного сообщения подлинным не должно быть ни одной ошибки ни в самом сообщении, ни в его имитовставке или цифровой подписи.

При использовании злоумышленником оптимизированных помех помехо-

устойчивость существующих методов аутентификации сообщений оказывается существенно ниже их помехоустойчивости при воздействии случайных помех. При имитозащищенной передаче сообщений злоумышленник, поразив помехой любую малую часть передаваемого сообщения, может оказаться способным добиться полного срыва связи. При этом принятое с некоторой ошибкой, но отвергнутое как имитонавязанное избыточное сообщение может иметь достоверность, вполне достаточную для получателя с точки зрения его требований к качеству видео-, речевого или телеграфного сообщения.

Решение задачи повышения помехоустойчивости методов обеспечения подлинности может быть найдено при построении систем аутентификации сообщений на основе водяных знаков. Под водяными знаками заверяемых сообщений понимаются их уникальные аутентификаторы, которые может опознать любой получатель сообщений, но которые может сформировать только отправитель аутентифицируемых сообщений, обладающий секретным ключом. Водяные знаки сообщений по своему назначению подобны цифровой подписи, но отличаются от нее тем, что являются устойчивыми к различным искажениям случайного и преднамеренного характера. В идеальной системе удалить водяной знак можно, только полностью разрушив само сообщение.

В настоящее время активно развиваются методы защиты подлинности на основе водяных знаков видео-, аудио-, речевых сообщений. Методы защиты на основе водяных знаков могут найти широкое применение в телекоммуникационных системах при передаче речевой и видеоинформации. Водяные знаки способны обеспечить контроль авторства и подлинности речевых сообщений, а также заверить изображения при видеоконференциях в условиях воздействия ошибок канала связи и попыток обмана со стороны злоумышленников. Заметим, что разработка методов, одновременно стойких к подделке и устойчивых к удалению водяных знаков, является сложной задачей.

Обобщим возможности и ограничения перечисленных систем защиты информации. При решении задачи сохранения в тайне передаваемых сообщений и информационного трафика системы шифрования способны обеспечить конфиденциальность сообщений, но потенциально не могут скрыть от злоумышленников факт их защищенной передачи. Системы шифрования, как уже было упомянуто, не согласованы с большинством реальных источников сообщений и каналов связи. В противоположность этому стеганографические системы потенциально способны сохранить в тайне и содержание, и факт передачи сообщений. Они могут быть построены с учетом характеристик источника сообщений и каналов их передачи. Эта возможность обусловлена тем, что стеганографические системы могут включать в себя кодер источника и кодер канала связи.

При обеспечении подлинности передаваемых сообщений известные криптографические системы аутентификации сообщений ориентированы преимущественно на защиту от подделки только информации, искажение которой в процессе обработки и передачи недопустимо, т. е. данных. Для заверенных данных допустим отказ от них при любых их искажениях. Однако для информации многих естественных источников информации, таких как речь и видео, некоторый

уровень искажений допустим. Для таких сообщений больше подходят системы аутентификации сообщений на основе водяных знаков, устойчивых к случайным и преднамеренным искажениям.

При защите авторских и иных прав на сообщения системы аутентификации сообщений на основе водяных знаков обеспечивают выявление неавторизованного использования защищаемой информации. Такие системы также позволяют связать каждый экземпляр сообщения с уникальным номером. Этот неудаляемый номер дает возможность отследить использование любого электронного сообщения. Такая возможность востребована при защищенном электронном делопроизводстве и при защите прав производителей различной информационной продукции.

Заключение

Таким образом, развитие и использование современных криптографических и стеганографических методов открывают новые возможности для защиты информации. Очевидно, что сложные задачи защиты информации от различных деструктивных действий злоумышленников могут быть решены при комплексном использовании различных методов ее защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Оков И.Н. Аутентификация речевых сообщений и изображений в каналах связи / под ред. В.Ф. Комаровича. – СПб. : Изд-во Политехн. ун-та, 2006. – 460 с.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М. : СОЛОН-ПРЕСС, 2009. – 272 с.

3. Комарович В.Ф., Оков И.Н., Корсунский А.С. Подход к построению сигнальной аутентификации корреспондентов сетей связи с подвижными объектами специального назначения // Проблемы совершенствования и развития специальной связи и информации, предоставляемых государственным органам: Сб. материалов 6-й Всерос. науч. конф. – Орел : Академия ФСО, 2007.

4. Корсунский А.С. Способ аутентификации вызовов корреспондентов в сетях подвижной радиосвязи с кодовым разделением каналов // сб. материалов 63-й науч. конф., посвященной Дню радио, НТОРЭС им. А.С. Попова. – СПб. : СПбГТУ «ЛЭТИ», 2008.

5. Корсунский А.С. Анализ протоколов аутентификации абонентских терминалов в сетях подвижной радиосвязи // Автоматизация процессов управления. – 2009. – № 4 (18). – С. 21–28.

6. Корсунский А.С., Шейкина О.В. Аутентификация в сетях UMTS при использовании псевдослучайных последовательностей Касами и Голда // Автоматизация процессов управления. – 2010. – № 2 (20). – С. 40–48.

7. Корсунский А.С., Ерышов В.Г. Защита инфотелекоммуникационных систем в условиях информационного противоборства // Автоматизация процессов управления. – 2011. – № 4 (26). – С. 82–85.

8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М. : ИПК Издательство стандартов, 1996.