5.Taubman D., Ordentlich E., Weinberger M., Seroussi G. Embedded block coding in JPEG 2000 // Signal Processing: Image Communication. 2002. №17. P. 49-72

6.Shoham Y., Gersho A. Efficient bit allocation for an arbitrary set of quantizers // IEEE Trans. Acoustics, Speech, and Signal Processing. 2000. № 9. P. 1445-1453.

7.Darmstaedter V., Delaigle J.-F., Quisquater J., Macq B. Low cost spatial watermarking // Computers and Graphics. 1998. Vol. 5. P. 417-423.

8.Langelaar G., Lagendijk R., Biemond J. Robust labeling methods for copy protection of images // Proc. Of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022.

УДК 004-681

Е.А..Кулагин

ОСОБЕННОСТИ ОРГАНИЗАЦИИ СТЕГАНОГРАФИЧЕСКИХ КАНАЛОВ В ПРОВОДНЫХ ТЕЛЕФОННЫХ ЛИНИЯХ

Что такое стеганографический канал? Это канал, который обеспечивает невидимую для сторонних наблюдателей передачу сообщений между отправителем и получателем.

Что такое невидимость? Это неспособность контролирующей системы осознать факт передачи сообщения между отправителем и получателем.

Невидимой может быть информация:

1) которая не вызывает осознаваемую контролирующей системой потерю информации в открытых сообщениях;

2) которая не может быть обнаружена по причине отсутствия у контролирующей системы методик или параметров необходимых для обнаружения;

3) которая в случае обнаружения не осознается контролирующей системой как нелегальная информация.

В какой степени необходимо обеспечить невидимость стеганографического канала? Достаточно ли будет обеспечить только первый из трех видов невидимости или необходимо совмещать два или все три вида невидимости информации? Все это зависит от способности контролирующей системы обнаруживать стеганографические каналы.

Что определяет способность контролирующей системы обнаруживать стеганографические каналы? Как доказывается в [1], способность системы видеть или не видеть оказываемое на нее воздействие определяется доминирующей в ней целью. Таким образом, определив пространство целей систем контроля, присутствующих на участке линии связи межу отправителем и получателем, можно определить некоторые особенности построения стеганографического канала для данного участка линии связи.

Структура стеганографического канала

В общем виде структура стеганографического канала описывается в многочисленной литературе, посвященной данной тематике, например [2].

В нашем случае необходимо рассмотреть особенности построения стеганографического канала при использовании различных точек подключения отправителя и получателя скрытого сообщения к телефонной линии связи.

Как известно, к телефонным линиям относятся абонентские линии и линии первичной сети [3]. Линии первичной сети должны хорошо охраняться, и подключение к ним связано с большими техническими трудностями, поэтому в данной статье этот участок не рассматривается.

Рассмотрим упрощенную структуру проводной телефонной линии связи (рис.1).

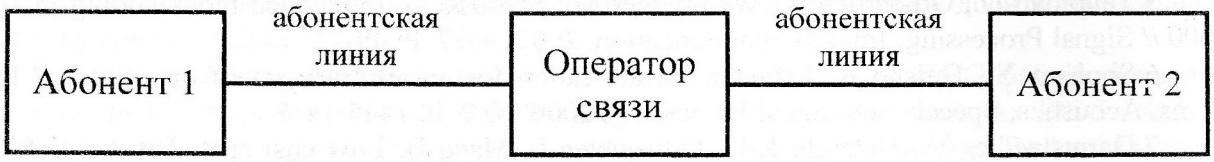

Рисунок 1. Структура телефонной линии связи

Из рисунка 1 можно сделать вывод, что существует два способа подключения отправителя и получателя к телефонной линии связи:

1) отправитель и получатель подключены к одной абонентской линии;

2) отправитель и получатель подключены к разным абонентским линиям.

Рассмотрим эти варианты.

Первый вариант показан на рисунке 2.

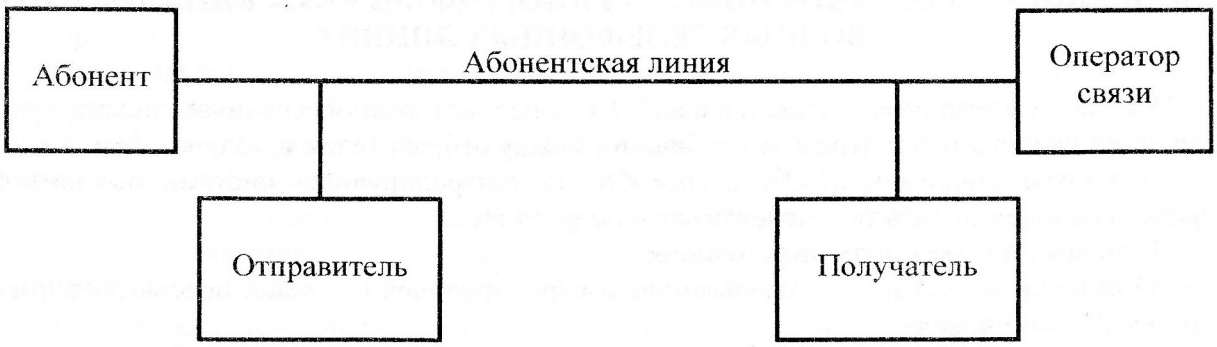

Рисунок 2. Передача сообщений по участку абонентской линии

В этом варианте отправитель и получатель используют только небольшую часть телефонной линии, а именно участок между АТС и абонентом. Недостатком такого способа подключения к телефонной сети является небольшая длина рабочего участка (не более 3 км), а также технические трудности подключения со стороны АТС. Достоинством является то, что данный участок линии неразрывный и может использоваться непрерывно. Кроме этого, между отправителем и получателем может отсутствовать оборудование оператора связи (за исключением проводов и кабелей), это позволит дополнительно изолировать скрытый канал путем установки отсекающих устройств в сторону абонента и оператора связи.

Второй вариант показан на рисунке 3.

Рисунок 3. Передача сообщений через коммутируемую сеть

В этом варианте стеганографический канал организуется в коммутируемой телефонной сети. Недостатком такой схемы является то, что сеанс передачи скрытого сообщения ограничивается длительностью сеанса связи абонентов, а так же тем, что параметры канала передачи ограничены параметрами низкочастотного канала тональной частоты.

Пространство целей контролирующих систем

После того как определена структура стеганографического канала, необходимо определиться с тем, кто же будет контролировать этот канал, какие цели при этом будет преследовать и как ему противодействовать.

Как видно из рисунков 2 и 3, на линии связи присутствуют только два объекта способные осуществлять контроль на наличие стеганографических каналов. Это абонент и оператор связи. Под абонентом будем понимать всех, кто подключается к телефонной линии как абонент, от глухой старушки до специалистов из органов контрразведки. Под оператором связи будем понимать любое оборудование, подключаемое со стороны АТС и между АТС от декадно-шаговых телефонных станций до сложных вычислительных и поисковых комплексов.

Какие цели, в области обеспечения безопасности технических систем передачи информации, может преследовать абонент?

1) Абонент может не интересоваться вопросами обеспечения безопасности и даже не знать об их существовании. Для такого абонента главное, чтобы телефон исправно работал. В этом случае к стеганографической системе на абонентском участке предъявляются минимальные требования: система не должна нарушать нормального функционирования телефонного канала. Система может изменять отдельные параметры линии (в пределах стандартных допусков на телефонные каналы), не влияющие на качество связи.

2) Абонент может преследовать цель защиты линии связи от несанкционированного подключения. Для этого он может установить устройства осуществляющие мониторинг электрических параметров линии и в случае изменения этих параметров вызывать специалистов, способных проводить поисковые мероприятия. В этом случае стеганографическая система может нарушать электрические параметры линии только в пределах допусков систем мониторинга.

3) Абонент может преследовать цели защиты своей информации. Для этого он может использовать различные системы скремблирования сигналов, зашумления и мониторинга линии. В этом случае стеганографическая система должна формировать сигналы, которые не будут вызывать подозрения в покушении на конфиденциальную информацию абонента.

4) Абонент может производить целенаправленный поиск стеганографических каналов информации или осуществлять меры активного противодействия. В данном случае стеганографическая система должна использовать методы сокрытия информации, превосходящие возможности стегоанализа.

Какие цели, в области обеспечения безопасности технических систем передачи информации, может преследовать оператор связи?

1) Оператор связи должен контролировать параметры линии с целью обеспечения абонента требуемым качеством телефонного канала. В данном случае стеганографическая система не должна изменять параметров линии более чем это допускается для оборудования абонента.

2) Оператор связи может производить мониторинг линии для защиты абонента от несанкционированных подключений. Особенности стеганографической системы здесь такие же, как и в предыдущем пункте.

3) Оператор связи может модифицировать передаваемую по линии информацию с целью увеличения пропускной способности линии (цифровая передача с компандированием, аппаратура высокочастотного уплотнения и т.п.), а также с целью защиты конфиденциальной информации абонента (шифрование). В данном случае необходимо использовать методы стеганографического преобразования не чувствительные к изменению параметров сигнала и работающие строго в рамках стандартного телефонного канала. Либо можно подключаться параллельно уплотненной абонентской линии (при передаче только на участке абонентской линии) с учетом особенностей организации данной цифровой линии связи.

4) Оператор связи совместно с органами контрразведки может производить мониторинг с целью обнаружения стеганографических каналов. В данном случае необходимо использовать весь арсенал средств противодействия стеганографическим атакам.

Заключение

Особенности организации стеганографических каналов в телефонных линиях связи определяются следующими условиями:

1) участком сети, на котором организуется скрытый канал:
   – участок абонентской линии;
   – коммутируемая телефонная сеть;
2) пространством возможных целей контролирующих систем:
   для абонента:
   – требование обеспечения качества связи;
   – защита от несанкционированного подключения;
   – защита своей информации;
   – защита от стеганографических каналов;
   для оператора связи:
   – обеспечение требуемого качества связи;
   – защита от несанкционированного доступа;
   – увеличение пропускной способности линии;
   – защита информации абонента;
   – защита от стеганографических каналов.

Анализ технических особенностей построения телефонных линий связи с учетом возможных целей контролирующих систем позволит создавать невидимые каналы передачи информации с минимальными затратами.

Список литературы

1. С.П. Расторгуев, Информационная война. – М.: Радио и связь, 1999.

2. В. О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук, Основи комп'ютерної стеганографії. Навчальний посібник – Вінниця: ВДТУ, 2003.

3. Городская телефонная связь. Справочник // под. ред. А.С. Брискера и .П. Мельникова, М.: «Радио и связь», 1987.

УДК 004.621

А.С. Петров, О.А.Талыкин

АНАЛИЗ УЯЗВИМОСТЕЙ WEB-СИСТЕМ

В настоящее время Web-системы все чаще используются для доступа к информационным ресурсам предприятий. Динамическое внедрения Интернет технологий во все сферы деятельности человека ставит особые требования к обеспечению безопасности Web-систем.

Построение защищенных Web-систем требует проведения анализа нарушения безопасности и выявления причин возникновения уязвимостей. Только знание природы этих причин позволяет оценить способность Web-систем противостоять атакам на ее безопасность, а так же понять природу недостатков существующих средств обеспечения безопасности.

Целью исследования является анализ нарушений безопасности Web-систем, выявление причин возникновения уязвимостей и их систематизация.