Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет

О.Ю. Пескова, Г. Ю. Халабурда

Технологический институт Южного федерального университета
poy@tsure.ru

Аннотация

В работе представлены основные понятия сетевой стеганографии, приведена классификация и рассмотрены базовые методы сетевой стеганографии. Приведена сравнительная таблица характеристик рассмотренных методов.

Введение

Сколько существуют глобальные сети, столько существует необходимость в скрытии как содержимого передаваемых данных, так и самого факта передачи информации.

Стеганография – наука о скрытой передаче информации. В отличие от криптографии, которая скрывает содержимое передаваемого сообщения и позволяет защитить конфиденциальность данных, стеганография прячет сам факт передачи сообщения. Если сообщение, защищённое методом стеганографии, не было обнаружено, то не будут обнаружены также отправитель и получатель. Можно использовать стеганографию в комплексе с криптографией для дополнительной защиты данных.

Интернет открыл массу возможностей для скрытой связи. Секретные сообщения могут быть скрыты не только в обычных открытых сообщениях, как в традиционной стеганографии, а также в элементах управления протоколов связи и в результатах изменения логики протокола.

В Интернет стеганография может применяться для самых разных целей – начиная от вполне безопасных и даже полезных, и заканчивая преступными. В частности, одно из наиболее востребованных «мирных» приложений стеганографии – защита авторского права, когда с помощью внедренного «водяного знака» можно доказать авторство материалов. Стеганографию можно использовать для цифровой маркировки материалов в электронных библиотеках и хранилищах. Стеганографическое вложение может в некоторой степени подменить собой электронную почту, потому что позволяет доказать целостность переданного материала. А с другой стороны, с помощью стеганографии инсайдер может передать через каналы Интернет закрытые данные, обходя все фильтры, установленные в сети организации. Стеганография может использоваться для скрытия факта передачи запрещенных материалов и для общения преступников и террористов. Поэтому методы стеганографии и стегоанализа требуют особо тщательного изучения.

Сетевая стеганография – вид стеганографии, в котором в качестве носителей секретных данных используются сетевые протоколы эталонной модели OSI - сетевой модели взаимодействия открытых систем. В общем виде сетевая стеганография является семейством методов по модификации данных в заголовках сетевых протоколах и в полях полезной нагрузки пакетов, изменению структуры передачи пакетов и гибридных методов в том или ином сетевом протоколе (иногда и нескольких сразу).

Передача скрытых данных в сетевой стеганографии осуществляется через скрытые каналы. Термин «скрытый канал» ввёл Simmons в 1983 году, который определил, что проблема утечки информации не ограничивается использованием программного обеспечения. Скрытый канал может существовать в любом открытом канале, в котором существует некоторая избыточность.

Скрываемые данные называются стеганограммой. Они располагаются в определенном носителе (carrier). В сетевой стеганографии роль носителя выполняет передаваемый по сети пакет.

Основные параметры сетевой стеганографии – это пропускная способность скрытого канала, вероятность обнаружения и стеганографическая стоимость. Пропускная способность - объём секретных данных, который может быть отправлен в единицу времени. Вероятность обнаружения определяется по возможности обнаружения стеганограммы в определенном носителе. Наиболее популярный способ обнаружить стеганограмму – это анализ статистических свойств полученных данных и сравнение их с типовыми значениями для этого носителя. Стеганографическая стоимость характеризует степень изменения носителя после воздействия на него стеганографического метода.

1. Классификация методов сетевой стеганографии

Исходными данными для рассмотрения классификации методов и средств сетевой стеганографии являются материалы польских учёных W. Mazurczyk и K. Szczypiorski, отчёты об экспериментах канадских учёных K. Ahsan и D. Kundur, учёных

Калифорнийского Университета в Ирвине E. Cauich, R. Gomez, исследователей Theodore G. Handel и Maxwell Sandford национальной лаборатории в LosAmos.

Методы сетевой стеганографии можно разделить на три группы (рисунок 1) [7]:

– методы стеганографии, суть которых в изменении данных в полях заголовков сетевых протоколах и в полях полезной нагрузки пакетов;
– методы стеганографии, в которых изменяется структура передачи пакетов, например, изменяются очередности передачи пакетов или преднамеренное введение потерь пакетов при их передаче;
– смешанные (гибридные) методы стеганографии — при их применении изменяются содержимое пакетов, сроки доставки пакетов и порядок их передачи.

Каждый из этих методов делится ещё на несколько групп; например, методы модификации пакетов включают в себя три разных метода:

– методы изменения данных в полях заголовков протокола: они основаны на модификации полей заголовков IP, TCP, SCTP и так далее;
– методы модификации полезной нагрузки пакета; в этом случае применяются всевозможные алгоритмы водяных знаков, речевых кодеков и прочих стеганографических техник по скрытию данных;
– методы смешанных техник.

Методы модификации структуры передачи пакетов включают в себя три направления:

– методы, в которых изменяется порядок последовательности пакетов;
– методы, изменяющие задержку между пакетами;
– методы, суть которых заключается во введении преднамеренной потери пакетов путём пропуска порядковых номеров у отправителя.

Смешанные (гибридные) методы стеганографии используют два подхода: методы потери аудио пакетов (LACK) [4] и ретрансляция пакетов (RSTEG) [7].

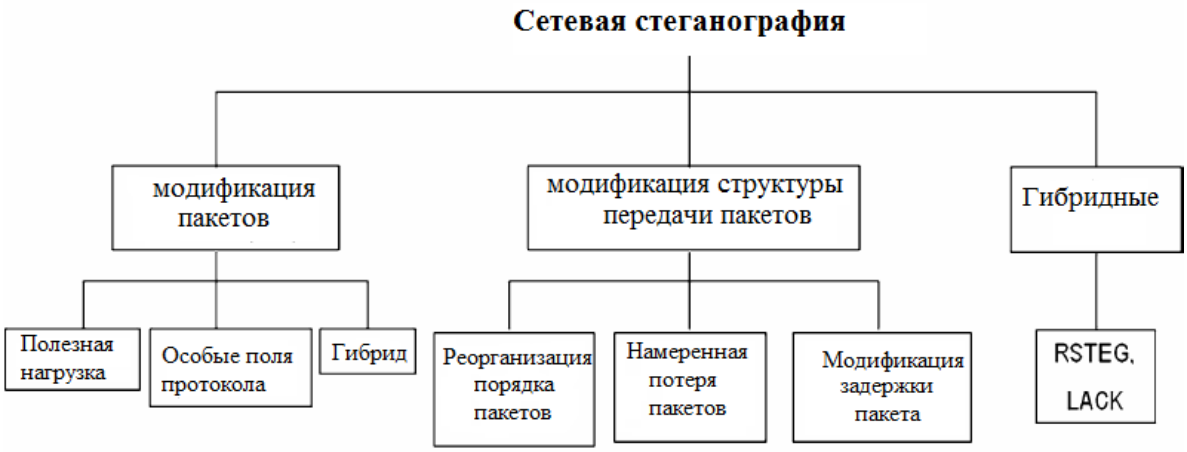

Рис.1 Классификация методов сетевой стеганографии

2. Методы сетевой стеганографии с модификацией пакетов

Главная идея методов модификации полей заголовков заключается в использовании некоторых полей заголовков для внесения в них стеганограммы [1, 2]. Это возможно за счёт некоторой избыточности в данных полях, то есть существуют определенные условия, в которых значения в данных полях не будут использоваться при передаче пакетов. Чаще всего используются поля заголовков IP и TCP протоколов.

Пример подобного метода, основанный на модификации полей заголовков протокола IP, приведен на рисунке 2.

Vers	Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Размер пакета	
Идентификатор Стеганограмма				Флаги	Смещение фрагмента
Время жизни		Протокол		Контрольная сумма заголовка	
Адрес Источника					
Адрес назначения					
Опции (если размер заголовка > 5)					
Данные					

Рис.2 Метод модификации полей IP-заголовка

В данном методе рассматривается модификация неиспользуемых полей для создания скрытого канала [2].

Значение поля Идентификатор (Identification) IP-пакета генерируется на стороне отправителя. Это число содержит случайный номер, который генерируется, когда создаётся пакет. Поле Identification используется только тогда, когда используется фрагментация. Поэтому для использования данного метода необходимо знать значение MTU в передаваемой сети и не превышать его, чтоб пакет не был фрагментирован во время передачи. При отсутствии необходимости фрагментации пакета, определенная избыточность возникает в поле «Флаги», во втором бите, отвечающем за установку флага Don'tFragment (DF). Существует возможность указать флаг, уведомляющий о нежелании отправителя фрагментировать пакет. Если пакет со стеганограммой не будет фрагментирован из-за его размера, можно скрыть информацию в поле флага DoNotFragmentBit. Использование данного метода предоставляет пропускную способность в 1 бит

Плюсом данного метода является передача без изменений информации от отправителя к получателю, но это также ограничивает количество посылаемой информации. Стеганография на основе данного метода является легко реализуемой, имеет неплохую пропускную способность, так как можно послать множество IP-пакетов с внесенными изменениями и низкую стоимость за счёт применения полей, не нарушающих функционала пакета. Если выбрать маршрут так, чтобы во время пути пакет не была фрагментирована, то данный метод может иметь вполне широкое применение за счёт указанных преимуществ. Из недостатков следует выделить то, что передаваемые данные содержатся в открытом виде и могут быть легко считаны наблюдателем (хотя можно усилить защиту, используя дополнительно криптографию).

Еще один метод модификации сетевых пакетов, изменяющий полезную нагрузку VoIP пакета, может найти широкое применение в практике за счёт популярности программ, обеспечивающих голосовую связь и видеосвязь через Интернет. Передача голоса по IP (VoIP или IP-телефония), является одной из услуг, которая позволяет пользователям делать звонки, передавая данные по сети с использованием IP-протокол. Метод сетевой стеганографии, предназначенный для скрытия сообщений VoIP, называется Transcoding Steganography (TranSteg)– метод сетевой стеганографии со сжатием полезной нагрузки сетевого пакета за счёт перекодирования. Данный метод может применяться для разнообразных мультимедийных классов и приложений реального времени, но его основное предназначение в приложениях IP-телефонии. TranSteg можно применять и в других приложениях или службах (например потоковое видео), там, где существует возможность сжатия (с потерями или без) открытых данных. Типичным подходом к стеганографии является сжатие данных, которое необходимо для ограничения размера передаваемых данных, ведь при использовании скрытого канала связи мы имеем ограниченную пропускную способность соединения. В TranSteg также используется сжатие данных, чтобы освободить место под стеганограмму: происходит перекодировка (сжатие с потерями) голосовых данных из высокого битрейта (занимающий больше места в полезной нагрузке пакета) в более низкий битрейт по возможности, с минимальной потерей качества голоса, и после сжатия происходит внесение данных в освободившееся место в области полезной нагрузки пакета [8]. В целом, метод позволяет получить более или менее хорошую стеганографическую пропускную способность в 32кб/с при наименьшей разнице в задержке пакета. Эксперименты польских учёных показали, что задержка в передаче VoIP пакета с использованием TranSteg возрастает на одну миллисекунду (1мс) в отличие от пакета без стеганограммы. Сложность обнаружения напрямую зависит от выбора сценария и условий постороннего наблюдателя (например, его расположения, в котором он может просматривать VoIP трафик). Из недостатков стоит упомянуть тот факт, что данный метод трудно реализовать. Нужно выяснить, какие кодеки использует программа для голосовой связи, подобрать кодеки с наименьшей разницей потери качества речи, при этом дающие больше места для вложения стеганограммы. При сжатии теряется качество передаваемой речевой информации.

Интересным представляется также направление с использованием механизмов SCTP-протокола. SCTP (Stream control transport protocol) [5] – транспортный протокол с контролем пакетов, транспортный протокол нового уровня, который заменит TCP и UDP в сетях будущего. Уже сегодня этот протокол реализуется в таких операционных системах как BSD, Linux, HP-UX и SunSolaris. Он также поддерживает сетевые устройства операционной системы CiscoIOS и может быть использован в Windows.

SCTP-стеганография использует новые характерные особенности данного протокола, такие как мультипоточность и использование множественных интерфейсов (multi-homing). Определенные новые угрозы и предложенные контрмеры могут быть использованы в качестве дополнения к RFC 5062, который описывает атаки в SCTP.

Методы SCTP-стеганографии можно разделить на три группы [6]:

– методы, в которых изменяется содержимое SCTP-пакетов;
– методы, в которых изменяется последовательность передачи SCTP-пакетов;
– методы, которые влияют как на содержание пакетов, так и их порядок при передаче (гибридный метод).

Методы изменения содержимого SCTP-пакетов основаны на факте, что каждый STCP-пакет состоит из частей, и каждая из этих частей может содержать переменные параметры.

Вне зависимости от реализации, статистический анализ адресов сетевых карт, используемых для пересланных блоков, может помочь в обнаружении скрытых связей. Устранение возможности примене-

ния данного метода стеганографии может быть достигнуто путём изменения адреса отправителя и получателя в случайно выбранном пакете, который содержится в повторно высылаемом блоке.

Суть гибридного метода на основе SCTP протокола заключается в использовании определенных механизмов протокола, которые позволяют организовать намеренный пропуск пакетов в потоке, без его повторной посылки. Позже в этот пакет добавляется стеганограмма, и он повторно отправляется [6].

Модификация пакетов с использованием гибридного метода может быть представлена на примере системы HICCUPS (Hidden Communication system for CorrUPted networkS), которая использует несовершенства передачи данных в сетевом окружении, такие как помехи и шум в среде связи, а также обычную подверженность данных к искажению [3]. HICCUPS является стеганографической системой с распределением пропускной способности в общественной сетевой среде. Беспроводные сети более восприимчивы к искажению данных, чем проводные, поэтому использование помех и шума в среде связи во время работы нашей системы выглядит очень заманчиво.

«Прослушка» всех кадров с передаваемыми данными в среде и возможность отправки поврежденных кадров с неправильно откорректированными кодовыми значениями – две важные сетевые особенности, необходимые для реализации HICCUPS. В частности, беспроводные сети используют воздушное соединение с переменной частой ошибок в битах (BER), что создаёт возможность вводить искусственно поврежденные кадры. В целом, новшества HICCUPS следующие:

– использование безопасных сетевых телекоммуникаций с криптографическими механизмами для обеспечения работы системы стеганографии;
– предложение нового протокола с распределением пропускной способности для стеганографических целей, основанных на испорченных пакетах.

Ключевой информацией с точки зрения систем скрытой связи является возможность обмена данными в скрытых каналах. Остальные каналы связи на уровне управления доступом к среде (MAC) открыты для криптоаналитической атаки и оставлены для проникновения в качестве наживки или приманки; эти каналы также служат для нормального обмена данными.

Данная система предназначена для общественных сетей, особенно для беспроводных локальных сетей. Этот метод обладает низкой полосой пропускания (зависит от сети), громоздкой реализацией, низкой стеганографической стоимостью и высокой сложностью обнаружения (если к существующей частоте ошибок кадра добавить 1%, как рассматривалось в примере). Тем не менее, анализ кадров с неверной контрольной суммой может привести к обнаружению использования данного метода.

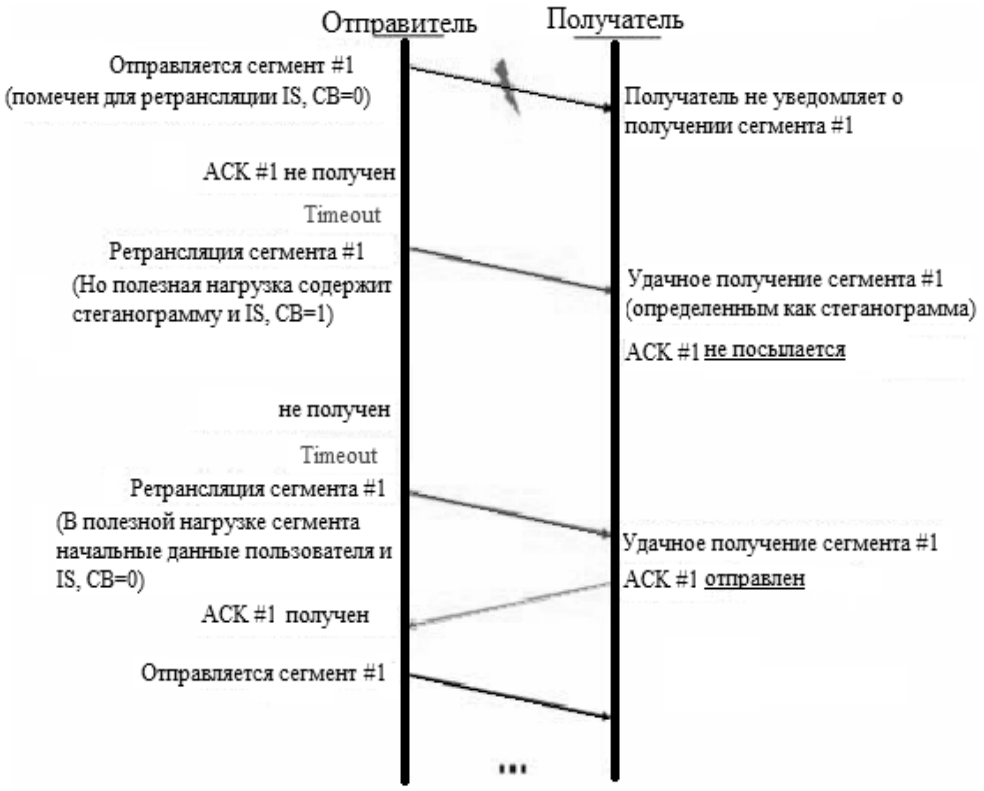

Рис. 3. Метод RSTEG

Таблица 2 Сравнение методов сетевой стеганографии

№	Пропускная способность стеганографии	Сложность обнаружения	Стоимость стеганографии	Реализация
1	TranSteg	HICCUPS	HICCUPS	Модификация полей в заголовках TCP и IP пакетов
2	LACK	TranSteg	LACK	Модификация блоков данных в SCTP протоколах
3	HICCUPS	LACK	RSTEG	TranSteg
4	RSTEG	RSTEG	TranSteg	Использование SCTP multi-homing
5	Модификация полей в заголовках TCP и IP пакетов	Использование протокола SCTP (гибрид)	Использование протокола SCTP (гибрид)	Использование протокола SCTP (гибрид)
6	Модификация блоков данных в SCTP протоколах	SCTP multi- homing	Модификация блоков данных в SCTP протоколах	LACK
7	Использование протокола SCTP (гибрид)	Модификация полей в заголовках TCP и IP пакетов	SCTP multi- homing	RSTEG
8	Использование SCTP multi- homing	Модификация блоков данных в SCTP протоколах	Модификация полей в заголовках TCP и IP пакетов	HICCUPS

3. Гибридные методы стеганографии

Метод RSTEG (рисунок 5) основан на механизме повторной посылке пакетов, суть которой заключается в следующем: когда отправитель посылает пакет, то получатель не отвечает пакетом с флагом подтверждения, и таким образом должен сработать механизм повторной высылки пакетов и повторно посылается пакет со стеганограммой внутри, на который также не приходит подтверждения. При следующем срабатывании данного механизма посылается оригинальный пакет без скрытых вложений, на который приходит пакет с подтверждением об удачном получении [7].

Производительность RSTEG зависит от многих факторов, таких как детали процедур связи (в частотности, размер полезной нагрузки пакета, частота, с которой генерируются сегменты и так далее). Ни один из реальных методов стеганографии не является совершенным. Независимо от метода, скрытая информация может быть обнаружена. В целом, чем больше скрытой информации внесено в поток данных, тем больше шансов, что она будет обнаружена, например, путем сканирования потока данных или другими методами стегоанализа.

Более того, чем больше пакетов используется для посылки скрытых данных, тем сильнее возрастает частота ретранслированных пакетов, чем существенно облегчает обнаружение скрытого канала связи. Именно поэтому процедура внесения скрытых данных должна быть тщательно подобрана и проконтролирована, чтобы свести к минимуму сложность обнаружения внесенных данных. К тому же, потери пакетов в сети должны быть тщательно проверены. RSTEG использует законный трафик, таким образом увеличивая общие потери. Чтобы убедиться, что общая потеря пакетов в сети нормальна и RSTEG не слишком высока по сравнению с другими соединениями в той же сети, уровень ретрансляции в целях стеганографии должен контролироваться и динамично адаптироваться.

Исследованный метод стеганографии с использованием ретрансляции пакетов RSTEG является гибридным. Поэтому его стеганографическая пропускная способность примерно равна пропускной способности методов с модификацией пакета, и при этом выше, чем у методов изменения порядка передачи пакетов .Сложность обнаружения и пропускная способность напрямую связана с использованием механизма реализации метода. RSTEG на основе RTO характеризуется высокой сложностью обнаружения и низкой пропускной способностью, а SACK обладает максимальной для RSTEG пропускной способностью, но и более легко обнаруживаем. Применение RSTEG возможно с использованием TCP протокола является хорошим выбором для IP-сетей. При разумном уровне преднамеренных ретрансляций не должен вызвать подозрений у наблюдателя. Из недостатков следует выделить тот факт, что данный метод сложно реализовать, особенно те его сценарии, которые основаны на перехвате и исправлении передаваемых обычными пользователями пакетов. Из-за резко возросшей частоты ретранслируемых пакетов или необычные возникновения задержек при передаче стеганограммы могут вызвать подозрения у стороннего наблюдателя.

LACK (Lost Audio Packets Steganography)– стеганография преднамеренных задержек аудио пакетов [4]. Это ещё один метод, осуществляемый через VoIP. Связь через IP-телефонию состоит из двух частей: сигнальной (дозвон) и разговорной. В обеих частях происходит передача трафика в обе стороны. Для передачи используется сигнальный протокол SIP и RTP (с RTCP, который выступает в роле управляющего протокола). Это значит, что в течении сигнальной фазы вызова конечные точки SIP (называемые пользовательские SIP агенты) обмениваются некоторыми SIP сообщениями. Обычно SIP сообщения проходят через SIP-сервера: прокси или перенаправленные, что позволяет пользователям искать и находить друг друга. После данного этапа начинается фаза разговора, где аудио (RTP) поток идёт в обоих направлениях между вызывающим и вызванным. Данный метод имеет определенные преимущества. Пропускная способность не меньше, а иногда и выше, чем у остальных алгоритмов, использующих аудио пакеты. Но при намеренном вызове потерь возникает ухудшение качества связи, что может вызвать подозрение или у обычных пользователей или у прослушивающего наблюдателя. Исходя из представленных методов стегоанализа LACK, можно заключить, что метод обладает средней сложностью обнаружения. Реализация метода слишком сложна, но может быть не возможна в пределах некоторых операционных систем.

Заключение

В таблице 2 приведено сравнение методов по их основным характеристикам и реализации. Позиция каждого метода в данной таблице показывает, на сколько его характеристики превосходят или уступают остальным. Чем выше отображен метод в таблице, тем больше показатели его характеристик. В поле Реализация рассматривается простота организации данного метода. Чем меньше времени и усилий требует реализация данного метода, тем выше его позиция данным заголовком. На основе данных из таблицы можно сделать вывод о прямой зависимости основных характеристик друг от друга.

Проведенные исследования могут быть использованы в качестве основы для разработки новых методов стеганографии или для защиты информации от утечек по скрытым каналам, созданных с помощью рассмотренных методов.

Литература

[1] Craig H. Rowland.Covert Channels in the TCP/IP Protocol Suite.- First Monday, Volume 2, Number 5 - 5 May 1997 [Электронный ресурс] / First Monday [сайт]. URL:http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/528/449 (дата обращения 13.09.2012).

[2] Enrique Cauich, Roberto Gómez ,Ryouske Watanabe. Data Hiding in Identification and Offset IP fields [Электронный ресурс]/ California University at Irwing, Computer Science and Engineering 204B University of California, Irvine, CA 92717 USA Sciweavers [сайт]. URL: http://www.sciweavers.org/read/data-hiding-in-identification-and-offset-ip-fields-124683 (дата обращения 13.09.2012).

[3] Szczypiorski K. HICCUPS: Hidden Communication System for Corrupted Networks-Międzyzdroje, Poland 2003 [Электронный ресурс] / Krzysztof Szczypiorski [сайт]. URL: http://krzysiek.tele.pw.edu.pl/pdf/acs2003-hiccups.pdf (дата обращения 13.09.2012).

[4] Mazurczyk W., Szczypiorski K. Steganography of VoIP streams.: In: MeersmanR, TariZ (eds) Springer-Verlag, 2009. [Электронный ресурс] / Wydziału Elektroniki i Technik Informacyjnych [сайт]. URL:http://home.elka.pw.edu.pl/~wmazurcz/moja/art/OTM_StegVoIP_2008.pdf (дата обращения 13.09.2012).

[5] Stewart R., Ed. Stream Control Transmission Protocol. -RFC 4960–Request for Comments: 4960, 2007 [Электронный ресурс] /IETF Tools [сайт]. URL:http://tools.ietf.org/html/rfc4960 (дата обращения 13.09.2012).

[6] W. Frączek, W. Mazurczyk, K. Szczypiorski. Stream Control Transmission Protocol Steganography. [Электронный ресурс] //Warsaw University of Technology, Institute of Telecommunications [сайт]. URL: http://arxiv.org/abs/1006.0247 (дата обращения 13.09.2012).

[7] Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski. Retransmission steganography and its detection. [Электронный ресурс] / IT2Net [сайт]. URL: http://cygnus.tele.pw.edu.pl

/~wmazurczyk/art/RSTEG.pdf (дата обращения 13.09.2012).

[8] Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski. Using Transcoding for Hidden Communication in IP Telephony. [Электронный ресурс] / Warsaw University of Technology, Institute of Telecommunications [сайт]. URL: http://arxiv.org/pdf/1111.1250v1.pdf (дата обращения 13.09.2012).

Application of network steganography for protection of the data transferred over the Internet

Olga Peskova, Georgy Halaburda

In paper the basic concepts of a network steganography are presented, classification is given and base methods of a network steganography are considered.. A comparative table of the characteristics of the methods is provided.