Вывод. Разработан метод распараллеливания алгоритма генерации ПСП на основе представления систем БФ посредством ЛЧП. Решение необходимо для построения высокопроизводительных средств криптографической защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бабаш, А.В., Шанькин Г.П.* Криптография / Под ред. В.П. Шерстюка, Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
2. *Тилборг.* Основы криптологии. – М.: Мир, 2006. – 472 с.
3. *Шнайер, Б.* Практическая криптография. – М.: Вильямс, 2005. – 424 с.
4. *Фороузан, Б.А.* Криптография и безопасность сетей: Учеб. пособие: пер. с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. – 784 с.
5. *Вишневский А.К., Финько О.А.* Реализация типовых функций гибридных криптосистем арифметико-логическими полиномами // Теория и техника радиосвязи. – 2011. – № 1. – С. 32-36.
6. *Вишневский А.К., Финько О.А.* Параллельная реализация систем подстановок числовыми полиномами // V Международная конференция «Параллельные вычисления и задачи управления» (PACO-2010). – М., 26-28 октября 2010.
7. *Диченко С.А., Вишневский А.К., Финько О.А.* Реализация двоичных псевдослучайных последовательностей линейными числовыми полиномами // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 130-140.
8. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов / В.Д. Малюгин. – М.: Физматлит, 1997. – 192 с.
9. *Финько, О.А.* Реализация систем булевых функций большой размерности методами модулярной арифметики // Автоматика и телемеханика. – 2004. – № 6. - С. 37-60.
10. *Yanushkevich L., Shmerko V., Lyshevski S.* Logic design of nanoICs. CRC Press, 2005.
11. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии: Учеб. пособие. – М.: Гелиос АРВ, 2001. – 480 с.

Статью рекомендовал к опубликованию д.т.н., профессор В.Н. Марков.

Диченко Сергей Александрович – Филиал Военной академии связи (г. Краснодар); e-mail: dichenko.sa@yandex.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79618588866; адъюнкт очной адъюнктуры.

Финько Олег Анатольевич – e-mail: ofinko@yandex.ru; тел.: +79615874848; профессор.

Dichenko Sergey Alexsandrovich – Branch of the Military Academy of Communications (Krasnodar); e-mail: dichenko.sa @yandex.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79618588866; associate postgraduate full-time.

Finko Oleg Anatolievich – e-mail: ofinko@yandex.ru; phone: +79615874848; professor.

УДК 81.93.29

О.Ю. Пескова, Ю. Г. Халабурда

ПРИМЕНЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ ДЛЯ СКРЫТИЯ ДАННЫХ, ПЕРЕДАВАЕМЫХ ПО КАНАЛАМ СВЯЗИ*

Представлены основные понятия сетевой стеганографии, приведена классификация и рассмотрены базовые методы сетевой стеганографии. Наиболее подробно проанализированы методы модификации полей заголовков, методы SCTP-стеганографии, а также гибридные методы. Приведена сравнительная таблица характеристик рассмотренных

* Работа поддержана грантом РФФИ №10-07-00464-а.

методов. Предложен комбинированный метод модификации полей IP и TCP заголовков, который не требует синхронизации по времени участников обмена скрытыми сообщениями и характеризуется низкой стоимостью стеганографии. Представлены достоинства, недостатки и ограничения предложенного метода.

Сетевая стеганография; криптография.

O.Yu. Peskova, Yu.G. Khalaburda

APPLICATION OF NETWORK STEGANOGRAPHY FOR PROTECTION OF THE DATA TRANSFERRED OVER THE INTERNET

In paper the basic concepts of a network steganography are presented, classification is given and base methods of a network steganography are considered. The most detailed analyzes methods of modification of header fields, methods, SCTP-steganography, and hybrid methods. The comparative table of characteristics of the methods is provided. We propose the combined method of modifying of the fields IP and TCP headers which doesn't require synchronization on time of participants of an exchange of the hidden messages, and is characterized by low cost of a steganography. This paper presents the advantages, disadvantages and limitations of the proposed method.

Network steganography; cryptography.

Введение. 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 г., 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. Методы 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. Все материалы находятся в свободном доступе.

Методы сетевой стеганографии можно разделить на три группы [1]:

- 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) [2] и ретрансляция пакетов (RSTEG) [1].

Главная идея методов модификации полей заголовков заключается в использовании некоторых полей заголовков для внесения в них стеганограммы [3, 4]. 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.

Рассмотрим пример подобного метода, основанный на модификации неиспользуемых полей протокола IP для создания скрытого канала [4].

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. 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. Метод сетевой стеганографии, предназначенный для скрытия сообщений VoIP, называется Transcoding Steganography (TranSteg)–метод сетевой стеганографии со сжатием полезной нагрузки сетевого пакета за счёт перекодирования. TranSteg можно применять и в других приложениях или службах (например потоковое видео), там, где существует возможность сжатия (с потерями или без) открытых данных. В TranSteg сжатие данных используется, чтобы освободить место под стеганограмму: происходит перекодировка (сжатие с потерями) голосовых данных из высокого битрейта 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 [5]. 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 1мс в отличие от пакета без стеганограммы. Сложность обнаружения напрямую зависит от выбора сценария и условий постороннего наблюдателя (например, его расположения). 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) [6] – 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, 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).

Методы SCTP-стеганографии можно разделить на три группы [7]:

- 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 применения 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 [7]. Модификация пакетов с использованием гибридного метода может быть представлена на приме-

ре 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 [8]. 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 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. Этот метод обладает низкой полосой пропускания (зависит от сети), громоздкой реализацией, низкой стеганографической стоимостью и высокой сложностью обнаружения. Тем не менее, анализ кадров с неверной контрольной суммой может привести к обнаружению использования данного метода.

Метод RSTEG основан на механизме повторной посылке пакетов, суть которой заключается в следующем: когда отправитель посылает пакет, то получатель не отвечает пакетом с флагом подтверждения, 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 [1]. 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).

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 с использованием TCP протокола является хорошим выбором для IP-сетей. 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 [2]. 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.

В табл. 1 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.

Таблица 1

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

2. Комбинированный метод с использованием модификации полей заголовков IP и TCP. Как уже было сказано ранее, методы модификации полей заголовков IP и TCP обладают определенными особенностями, которые выделяют их на фоне остальных методов:

- в качестве носителей стеганограммы используются самые распространённые и стандартные протоколы;
- в сумме дают пропускную способность 49 бит за 1 пакет;
- реализуются на любой операционной системе, реализация не требует долгих настроек и подготовок;
- изменения в пакете не повлияют на его поведение в сети, в случае, если он не будет фрагментирован.

Несмотря на многие достоинства обоих методов, присутствуют и некоторые недостатки, и главный из них, на который сразу обращается внимание, – это явность передачи данных, т.е. любой статистический анализ позволяет вычислить как сам скрытый канал связи, так и передаваемую в нём информацию.

Предложенный Крейгом Ролландом [3] метод заключается в следующем: для генерации значения в поле «Номер последовательности» зашифровывается символ открытого текста в соответствии с таблицей ASCII, и полученное значение умножается на определенное число, кратное двум. Полученное значение вносится в поле «Номер последовательности» и отправляется получателю. Получатель, зная ключ (делитель), должен проверять все входящие TCP пакеты на предмет стеганограммы, производя деление значения поля «Номер последовательности» на ключ. С одной стороны, данный метод позволяет создавать канал данных, благодаря которому можно передавать секретные данные на виду у пассивного наблюдателя. Но существование одного ключа и является недостатком, так как на основе десятка таких пакетов можно сделать вывод, что порядковые номера всех пакетов имеют общий множитель, который и является ключом. Таким образом, предложенный метод легко обнаружить.

Отталкиваясь от исходных данных и анализа недостатков методов сетевой стеганографии с модификацией полей заголовков IP и TCP пакетов, можно предложить модифицированный метод, который будет основан на одновременном использовании полей заголовка IP и TCP протоколов. Ключ, необходимый для расшифровки передаваемого сообщения, будет также передаваться, как стеганограмма, только в зашифрованном виде в поле «Идентификатор» IP заголовка, в то время как зашифрованная стеганограмма будет передаваться в поле «Номер последовательности» TCP заголовка.

Реализация данного метода делится на две части:

1. Подготовка данных для передачи, которая включает в себя генерацию ключа k, преобразование передаваемого секретного символа или числа в соответствующий ему код в таблице ASCII и подсчёт значения носителя C, которое представляет собой зашифрованную стеганограмму.
2. Внесение данных в соответствующие поля заголовков TCP и IP.

Первый блок состоит из следующих шагов:

1. Генерация ключа k, который будет использоваться в дальнейшем. Ключом может быть любое число, кратное двум. Для генерации ключа возьмём два числа x и y и первое возведем в степень второго.
2. Преобразование секретных данных – символа или числа, которые необходимо передать, в соответствующий ему код в таблице ASCII. Кодированное число обозначим как S, так как оно является нашей стеганограммой.
3. Получение носителя C как произведение значения ключа на значение кода секретного символа.

$$C = S*k_{10}$$

4. Проверка числа C – оно должно удовлетворять требованию $2^{28}<C<2^{33}$. Данное условие необходимо для того, чтобы значение поля «Номер последовательности» не выглядело подозрительно. Если значение C не отвечает предъявленным требованиям, числа x и y необходимо изменить на другие и повторить шаги 1-2. В дальнейшем будут проведены исследования по автоматическому формированию x, y.
5. Значение чисел x и y записывается слитно в число z и переворачивается так, чтобы прежние значение можно прочитать только справа налево, после чего преобразуется из десятеричной системы счисления в шестнадцатеричную. Таким образом, мы получаем трёхзначное шестнадцатеричное число $\mathrm{inv}(z)_{16}$.

Далее, на втором этапе, нужно внести полученные значения зашифрованного ключа и стеганограммы в поля заголовков TCP и IP.

Кратко опишем метод сетевой стеганографии с модификацией полей в TCP заголовке, так как в нём мы будем передавать само секретное сообщение. В заголовке этого протокола в целях стеганографии обычно используют некоторые поля, которые можно изменить без потери функциональности пакета. В целях нашего исследования остановимся на поле «Номер последовательности» (SN-SequenceNumber). Это поле выполняет две задачи. Первая заключается в следующем: если установлен флаг SYN, то это начальное значение номера последовательности – ISN (InitialSequenceNumber), и первый байт данных, которые будут переданы в следующем пакете, будет иметь номер последовательности, равный ISN + 1. В противном случае, если SYN не установлен, первый байт данных, передаваемый в данном пакете, имеет этот номер последовательности. Для нашего случая важно знать, что данное значение не изменится за время пути пакета от отправителя до получателя.

Поле «Номер последовательности» позволяет создавать последовательность длиноq в 32 бита. По методу Роуланда, передаваемое сообщение кодируется в соответствии с таблицей ASCII и умножается на определенное число (ключ), кратное двум для понижения вероятности обнаружения, затем вносится в генерируемый TCP пакет в поле «Номер последовательности» и пакет отправляется. При достижении пакетом адреса назначения, получатель должен сохранить все пришедшие TCP пакеты, из которых он должен изъять значение в поле «Номер последовательности», после чего поделить на заранее известный ему ключ. Но, как было раньше сказано, данный метод крайне легко обнаружить на основе анализа ряда TCP пакетов из-за постоянного ключа. В предлагаемой модификации метода данный ключ будет передаваться одновременно с TCP пакетом, в IP заголовке. Это повысит сложность обнаружения стеганограммы.

Следующим действием будет внесение значения носителя C в поле «Номер последовательности» TCP заголовка.

Далее необходимо внести значение зашифрованного ключа $(\mathrm{inv}(z))_{16}$ в поле IP заголовка. Для организации подобной операции следует вернуться к методу сетевой стеганографии с модификацией полей IP заголовка. Неизменными во время пути пакета остаются только поле «Идентификатор», длина которого составляет 16 бит, и 1 бит в поле «Флаги», отвечающий за флаг DF (Donotfragment – не фрагментировать). Изменение данных полей не несёт изменений в пакете, в случае, если не будет производиться фрагментация пакета, а её быть не должно, так как по условию мы должны знать минимальное значение MTU и не превышать его при создании и отправке пакета.

В поле «Идентификатор» нам доступно 16 бит для добавления стеганограммы, информация в нём отображается в виде четырёх чисел в шестнадцатеричной системе счисления. Таким образом, в нашем распоряжении 65535 возможных значений, которые можно использовать как для передачи стеганограммы, так и для ключа, который в свою очередь тоже является стеганограммой. Чтобы не передавать ключ в столь явном виде, предлагается использовать только три числа из четырёх, при этом считывая их справа налево. В таком случае число может быть и нечётным при стандартном его прочтении слева направо. Четвёртое неиспользуемое число может принимать любое значение. Таким образом, мы можем использовать только 16 из 17 доступных в пакете бит. Предлагается использовать второй бит в поле «Флаги» – DF (не фрагментировать) в качестве определенной метки, наличие которой позволяет расширить алгоритм извлечения ключа: нужно ли читать значение с первого или со второго числа в поле «Идентификатор» для извлечения ключа.

Таким образом, следующим шагом становится внесение (inv(z))16 в поле «Идентификатор» IP заголовка. При этом, мы должны выставить значение “1” второму биту в поле «Флаги», если мы вносим ключ в первые 12 байт поля «Идентификатор» или 0, если мы заполняем первые 4 байта поля случайными значениями, а в оставшиеся 12 байт вносится наш ключ.

Далее мы отправляем пакет с модифицированными полями получателю, где он должен провести процедуру, обратную описанной в рамках данного алгоритма.

Произведем расчет пропускной способности предложенного метода.

Так как поле «Идентификатор» в IP заголовке может содержать 16 бит информации, в поле «Флаги» доступен 1 бит, а в поле «Номер последовательности» в TCP заголовке доступен объём информации в 32 бита можно сделать вывод, что общая пропускная способность стеганографии равна 49 битам. Но следует отметить, что в данном методе мы используем поле «Идентификатор» для передачи зашифрованного ключа в стеганограмме, который служит для извлечения секретной информации из поля «Номер последовательности», а бит в поле «Флаги» используется в качестве метки. Таким образом, для передачи зашифрованного ключа мы выделяем 12 бит информации, доступные в поле «Идентификатор», в оставшиеся 4 бита мы вносим случайное число от 0 до 16 в шестнадцатеричной системе счисления (от 1 до F) и используем 1 бит в качестве метки, необходимой для более организации более гибкой работы алгоритма. Исходя из этого, можно сделать вывод, что для передачи конкретной информации у нас остаётся 32 бита в поле «Номер последовательности», и можно передать 3 бита секретной информации, которая зашифрована в 32 бита информации, скрывающей секретную.

Заключение. Представленный метод объединяет в себе два базовых метода (модификации полей IP и TCP заголовков), то есть включает в себя их достоинства, но при этом обладает более высокой сложностью обнаружения, и, как следствие, более стоек к статистическому стегоанализу. Метод не требует синхронизации по времени участников обмена скрытыми сообщениями и характеризуется низкой стоимостью стеганографии.

В данном методе присутствуют некоторые ограничения и недостатки, такие как:

- необходимость избегать фрагментации пакета, используемого в целях стеганографии;
- низкая пропускная способность данного метода.

Следует также отметить некоторые ограничения, которые стоит учитывать ещё перед генерацией пакета, в процессе подбора чисел, необходимых для генерации ключа. Кроме того, желательно провести дополнительные исследования с точки зрения устойчивости метода к стегоанализу.

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.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski.* Retransmission steganography and its detection. – Электронный журнал [Электронный ресурс]. – Режим доступа: http://cygnus.tele.pw.edu.pl /~wmazurczyk/art/RSTEG.pdf свободный
2. *Mazurczyk W., Szczypiorski K.* Steganography of VoIP streams.:электронный журнал [Электронный ресурс]. – In: MeersmanR, TariZ (eds) Springer-Verlag, 2009. – Режим доступа:http://home.elka.pw.edu.pl/~wmazurcz/moja/art/OTM_StegVoIP_2008.pdf, свободный.
3. *Craig H.* Rowland.Covert Channels in the TCP/IP Protocol Suite. – First Monday. – 1997. – Vol. 2, № 5: Электронный журнал [Электронный ресурс]. Режим доступа: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/528/449, свободный.
4. *Enrique Cauich, Roberto Gómez, Ryouske Watanabe.* Data Hiding in Identification and Offset IP fields. Электронный журнал[Электронный ресурс]. – California University at Irwing, Computer Science and Engineering 204B University of California, Irvine, CA 92717 USA. – Режим доступа: http://www.sciweavers.org/read/data-hiding-in-identification-and-offset-ip-fields-124683, свободный.
5. *Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski.* Using Transcoding for Hidden Communication in IP Telephony.-электронное пособие [Электронный ресурс]. – Warsaw University of Technology, Institute of Telecommunications. 2011. – Режим доступа: http://arxiv.org/pdf/1111.1250v1.pdf, свободный.
6. *Stewart R.* Ed. Stream Control Transmission Protocol. – RFC 4960: Электронный документ [Электронный ресурс]. – Request for Comments: 4960, 2007. – Режим доступа: http://tools.ietf.org/html/rfc4960, свободный.
7. *Frączek W., Mazurczyk W., Szczypiorski K.* Stream Control Transmission Protocol Steganography. – Электронное пособие [Электронный ресурс]. – Warsaw University of Technology, Institute of Telecommunications. 2010. – Режим доступа: http://arxiv.org/abs/1006.0247, свободный.
8. *Szczypiorski K.* HICCUPS: Hidden Communication System for Corrupted Networks. – Электронный доклад [Электронный ресурс]. – Międzyzdroje, Poland 2003. – Режим доступа: http://krzysiek.tele.pw.edu.pl/pdf/acs2003-hiccups.pdf, свободный.

Статью рекомендовал к опубликованию к.т.н. А.С. Басан.

Пескова Ольга Юрьевна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: poy@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; к.т.н.; доцент.

Халабурда Георгий Юрьевич – e-mail: headballz@yandex.ru; студент.

Peskova Olga Yur'evna – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: poy@tsure.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security of information technologies; cand. of eng. sc.; associate professor.

Khalaburda Georgy Yur'evich – e-mail: headballz@yandex.ru; student.