ПРИМЕНЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ ЗЛОУМЫШЛЕННИКАМИ ДЛЯ СКРЫТОГО ОБМЕНА ИНФОРМАЦИЕЙ И ОСУЩЕСТВЛЕНИЯ КОМПЬЮТЕРНЫХ АТАК

М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, fedosenkomaksim98@gmail.com;*
А.В. Агарков, *Национальный исследовательский университет ИТМО, a1sk8te@yandex.ru.*

УДК 004.056

Аннотация: Сфера кибербезопасности непрерывно развивается, поскольку злоумышленники постоянно ищут новые и изощренные способы нарушения целостности, конфиденциальности и доступности систем и сетей. Одним из таких способов является применение методики сетевой стеганографии, при помощи которой скрытые данные передаются законными путями, с использованием легитимных сетевых соединений. В данной работе исследуются методы сетевой стеганографии, которые применяются для передачи и вложения стеганограммы в сетевые пакеты.

Ключевые слова: сетевая стеганография; сети; сетевые протоколы; скрытая передача данных; *TCP/IP*.

APPLICATION OF NETWORK STEGANOGRAPHY BY CRIMINALS FOR HIDDEN INFORMATION EXCHANGE AND IMPLEMENTATION OF COMPUTER ATTACKS

M. Fedosenko, *National Research University ITMO;*
A. Agarkov, *National Research University ITMO.*

Annotation. The cybersecurity is constantly evolving because attackers continually seek new and sophisticated ways to compromise the integrity, confidentiality, and availability of systems and networks. One such method is the use of network steganography techniques, in which hidden data is transmitted to legitimate ways, using network connections. This paper contains network steganography methods that are used to transmit and embed steganograms in network packets.

Keywords: network steganography; networks; network protocols; hidden data transmission; *TCP/IP*.

Введение

Сетевая стеганография – это методика, которая используется злоумышленниками для скрытого обмена информацией, позволяющая спрятать данные внутри обычных, часто используемых легальных сетевых соединений. Такая концепция скрытой передачи делает передачу данных почти невидимой для систем безопасности. Важно, чтобы отправитель и получатель знали о процессе стеганографии, поскольку для стороннего наблюдателя такая передача данных является вполне законной, даже при неглубоком анализе трафика. Информация, вложенная в полезную нагрузку пакета и передаваемая с помощью стеганографии, называется стеганограммой. Процедура, которая анализирует пакеты в сетевом трафике на обнаружение стеганографии и наличия стеганограмм называется стегоанализом.

Сетевой пакет, это основной юнит, используемый для передачи данных по сети. Он представляет из себя контейнер, содержащий передаваемую информацию от одного устройства в сети к другому. Независимо от использования протокола

сетевой пакет может содержать основные поля, например, поле заголовка, полезной нагрузки, адреса отправителя и адреса получателя и т.д. Некоторые из этих полей могут включать полезную информацию, передаваемую при обмене пакетами между системами. Кроме этого, пакеты могут разбиваться, т.е. фрагментироваться, в зависимости от используемого протокола. Это позволяет не превышать размер ограничения *MTU* (максимальная единица передачи), не вызывая тем самым ограничения пропускной способности сети, и потерю пакетов, которая приводит к задержке и потери данных.

Такую архитектуру передачи данных по сети активно используют злоумышленники, чтобы передавать скрытые данные в легитимных пакетах. Согласно *MITRE ATTACK* [1] сетевая стеганография относится к классу обфускации данных под идентификатором T1001.002 и включает в себя 11 техник, применяемых для передачи стеганограммы по сети.

Целью данного исследования является рассмотрение различных методов вложения и передачи стеганографической информации с помощью сетевого трафика, а также установление особенностей изменения сетевых пакетов для последующей реализации механизмов защиты сетевой инфраструктуры от скрытых атак, реализованных посредством вредоносных вложений в пакеты.

Реализация поставленной проблемы предполагает следующие задачи:

- Классификация методов сетевой стеганографии в зависимости от механизмов сокрытия данных внутри трафика.
- Литературный анализ научных работ по исследуемой тематики с целью выделения и обобщения случаев и особенностей практического применения сетевой стеганографии.
- Определение сетевых протоколов модели *OSI*, позволяющих сокрытие данных и степени возможностей практического осуществления сокрытия и последующего обмена стеганографией.
- Сравнительный анализ полученных методов.

Методы сетевой стеганографии

В целом методы сетевой стеганографии можно разделить на три большие группы:

- Методы, изменяющие данные в полях заголовков сетевых протоколов.
- Методы, изменяющие структуру передачи сетевых пакетов.
- Гибридные методы, основанные на изменении содержимых пакетов, структуру передачи и сроков доставки.

В работе [2] исследуется метод вставки секретных данных в фрагменты пакета на основе идентифицирующей последовательности (*IS*). Идентифицирующая последовательность в данном методе применяется для того, чтобы различать стеганографические фрагменты от обычных, увеличивая сложность обнаружения таких фрагментов. При этом *IS* содержит дополнительные значения смещения фрагмента и номер идентификации фрагмента. Идентифицирующая последовательность заранее составляется с помощью хэш-функции отправителем и получателем. Далее, передача стеганограммы принимает следующий вид:

1. Отправитель добавляет секретные данные в полезную нагрузку фрагмента *IP*-пакета.

2. Вычисляется *IS* с помощью хэш-функции с заранее известным *Steg*-ключом и добавляется в полезную нагрузку фрагмента.

3. На принимающей стороне на основе значения *Steg*-ключа вычисляется *IS*.

4. Пакет извлекается, если *IS* в его полезной нагрузке совпадает с вычисленной на предыдущем этапе.

Значения в полях смещения фрагмента и идентификации остаются такими же, как и в других допустимых фрагментах. Пример метода изменения фрагментов представлен на рис. 1 (*H* – заголовок, *P* – полезная нагрузка, *S* – секретные данные), где: *Steganography Sender* (*SS*) является отправителем стеганограммы и источником фрагментации, а *Recipient of Steganography* (*SR*) получателем.

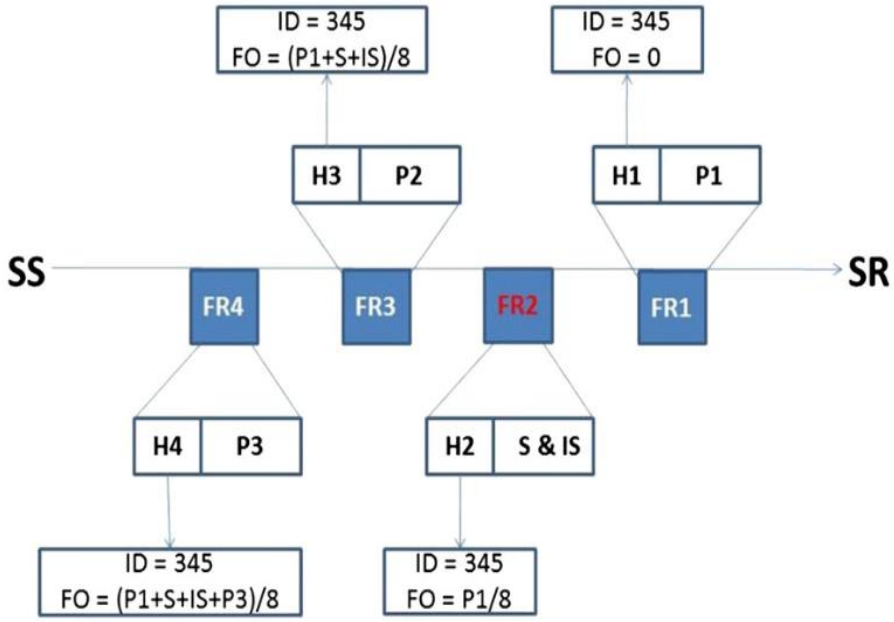

Рисунок 1

Помимо метода изменения фрагмента, в работе [2] авторы приводят пример метода модуляции числа фрагментов, который основан на изменении структуры передачи пакетов путем вставки скрытого бита. *SS* добавляет один бит данных, разделяя, таким образом, каждый из *IP*-пакетов на предопределенное количество фрагментов. В зависимости от ранее обговоренного способа обнаружения стеганографии *SR* может считывать передаваемую стеганограмму, как показано на рис. 2.

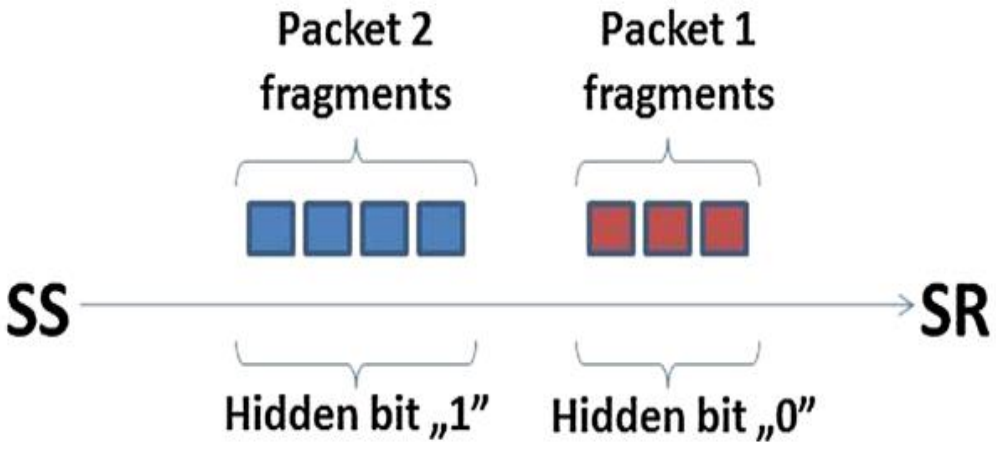

Рисунок 2

Алгоритм работы данного метода следующий:

1. Отправитель разбивает *IP*-пакет на множество фрагментов.
2. Четное количество фрагментов означает передачу двоичного «0».
3. Нечетное количество фрагментов означает передачу двоичной «1».
4. Извлечение данных из трафика основано на заранее обговоренном количестве пакетов.

В работе [3] также рассматривается этот метод, недостатком которого является ограниченное количество информации, передаваемой таким образом и легкость в обнаружении. Однако, авторы работы [2] предлагают решение проблем, связанных с использованием этого метода путем объединения с методом изменения фрагментов и применения их одновременно к общему носителю, в виде сетевого протокола.

В работе [4] исследуется гибридный метод стеганографии, который включает в себя изменение сетевого пакета и структуры передачи пакетов. Метод основан на принудительной потере пакетов *Lost Audio Packets* (*LACK*) и используется в технологиях телефонии, например, *VoIP* при передаче пакетов протокола *Real-time Transport Protocol* (*RTP*). Принцип работы данного метода, следующий:

1. Выбирается один пакет *RTP* из голосового потока.
2. Полезная нагрузка выбранного *RTP*-пакета заменяется секретным сообщением.
3. Выбранный пакет намеренно задерживается перед передачей.
4. Пакет распознается как чрезмерно задержанный и извлекается стеганограмма.

SS намеренно задерживает некоторые выбранные *RTP*-аудиопакеты перед передачей. Пакеты отбрасываются на стороне *SR*, если задержка таких пакетов в приемнике считается чрезмерной, а также отбрасываются в том случае, если получатель не осведомлен о процедуре стеганографии. Голосовая полезная нагрузка фрагмента заменяется битами стеганограммы в соответствии, например, с методом на основе изменения фрагмента, как показано на рис. 3.

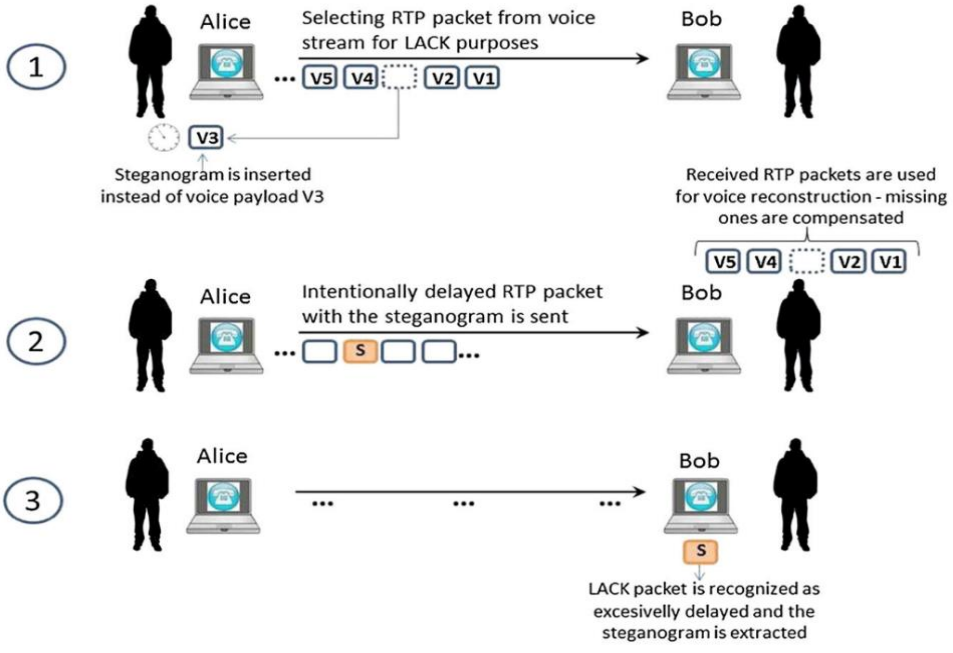

Рисунок 3

Однако, данный метод имеет недостатки, связанные с качеством передаваемой информации, которая ухудшится, если будет задержано слишком много *RTP*-пакетов, в результате этого выполнение стеганоанализа будет тривиальным. Как сообщают авторы исследования [3], данный метод обладает средней сложностью обнаружения и имеет сложную реализацию, зависящую от определенных операционных систем.

Как показывают авторы [2], метод можно улучшить при соблюдении осторожности во время выбора *RTP*-пакетов. В целях уменьшения общего уровня потери пакетов и в соответствии с условиями сети, высока вероятность не достигать определенного порога обнаружения.

В качестве меры оценки методов авторами исследования [2] была предложена стеганографическая стоимость. Данная характеристика выражает степень изменения носителя информации. Изменением может являться потеря определенной функциональности или ухудшение качества передаваемой информации протоколом после воздействия на него стеганографического метода.

Метод, основанный на модуляции числа фрагментов, имеет довольно низкую стоимость, поскольку его применение не затрагивает поля, нарушающие функционал пакета и его достаточно просто реализовать. Однако метод вносит неравномерности в количество фрагментов в пакете. В свою очередь, метод изменения фрагментов, основанный на *IS* влияет на скорость передачи данных носителем, поскольку применение метода увеличивает общее количество фрагментов пакета. Данный метод можно считать менее обнаруживаемым по сравнению с методов модуляции числа фрагментов. Уже упомянутое комбинирование этих методов уменьшает общую стоимость стеганографии по сравнению со стоимостью методов по отдельности. Такой эффект называется суперпозицией стеганографии.

На основе принципа работы метода *LACK* можно сделать вывод, что метод имеет довольно высокую стоимость, выражающуюся в чувствительности к потере пакетов из-за использования некоторых пакетов для передачи стеганограммы.

Злоупотребление такими потерями может привести к снижению качества передаваемой информации для пользователей. Например, потеря пакетов должна быть не выше 0,3% от общего числа пакетов, чтобы свести к минимуму стоимость и избежать возможности обнаружения.

Сравнительный анализ описанных методов представлен в табл. 1.

Таблица 1.

Метод	**Достоинства**	**Недостатки**	**Особенности**
Изменения фрагментов	1. Сложность стеганоанализа за счет неизменности общего числа фрагментов и их внешнего вида. 2. Дополнительная защита стеганограммы хэш-функцией с заранее известным *Steg*-ключом. 3. Простота реализации.	1. Различие хэш-значения от полученного от исходных данных без вложения 2. Геометрическое распространение ошибок в результате изменения содержимого пакета	Обеспечивает практическую неизменность общего вида сетевого трафика, за исключением состава пакета и его хэша, что можно обнаружить методом целенаправленного получения хэш-значения для исходных данных без вложения.

Метод	Достоинства	Недостатки	Особенности
Модуляции числа фрагментов	1. Низкая «стоимость» реализации. 2. Не затрагивает структуру и вид отдельного пакета.	1. Ограниченный объем вложенной информации. 2. Легкость обнаружения. 3. Сложность реализации.	Основан на изменении структуры передачи пакетов, в результате чего число пакетов зависит от передаваемой стеганограммы, что приводит к видоизменению трафика и повышает обнаруживаемость.
Lost Audio Packets (LACK)	1. Возможность передачи стеганограммы за счет временных характеристик, при помощи задержки пакетов. 2. Снижения уровня обнаруживаемся за счет использования комбинированного подхода.	1. Высокая «стоимость» реализации. 2. Низкий процент содержания измененных (стеганографичеких пакетов) за счет чувствительности к потерям пакетов. 3. Реализация зависит от операционной системы.	Гибридный метод, основанный на особенностях видоизменения трафика двух предыдущих и применяемый непосредственно в объемных пакетах телефонии.

Таким образом, объединение нескольких стеганографических методов на одном носителе может снизить общую стоимость стеганографии, что положительно влияет на успешность передачи скрытой информации и уменьшение вероятности ее обнаружения. Также авторы [2] отмечают, что на объединение методов могут потребоваться вычислительные, ресурсные и временные затраты. Однако объединение без каких-либо дополнительных затрат является частным случаем суперпозиционной стеганографии и называется стеганографией с нулевыми затратами.

Сетевые протоколы

Для работы со стеганографией можно применять любые популярные сетевые протоколы, которые будут выступать в роли носителя стеганограммы. Для вставки стеганограммы существуют особые условия изменения полей пакета сетевых протоколов. Поскольку данные поля являются необязательными, то их изменение не окажет влияние на качество передачи данных, однако эти поля можно использовать для скрытой передачи информации, чем успешно пользуются злоумышленники, передавая стеганограммы в компьютерных сетях. В работах [5] и [6] приводится исследование множества различных популярных протоколов, таких как *TCP, UDP, IP*. В работах описываются поля, которые можно применять для сетевой стеганографии.

Протокол *Transmission Control Protocol* (*TCP*) используется для надежной передачи данных между устройствами, который гарантирует доставку пакетов данных между клиентом и сервером в правильной последовательности без потерь. Главными полями, данные в которых могут быть заменены на стеганограмму в этом протоколе являются: поле указатель важности (*Urgent pointer*), поле опции (*Option*), поле порядковый номер (*Sequence Number*), поле контрольная сумма (*Checksum*).

Протокол *User Datagram Protocol* (*UDP*) является протоколом транспортного уровня и используется при передачи большого объема данных в сети, не гарантируя при этом доставку клиентом или подтверждение получения пакетов со стороны сервера. Он является быстрее протокола *TCP* и необходим в средах, где небольшие задержки не сильно критичны. Поля, которые могут заменить свою полезную нагрузку в этом протоколе выступают: поле порт отправителя (*Source port number*), поле *Checksum.*

Интернет-протокол версии 4 (*IPv*6) – это протокол сетевого уровня, который используется для маршрутизации и доставки пакетов с полезной нагрузкой в сети Интернет. Принцип работы протокола основан на определении уникальных *IP*-адресов для каждого устройства в сети Интернет и формировании пакетов для передачи. Полями, которые можно использовать для передачи стеганограммы являются: поле указатель перегрузки (*Explicit Congestion Notification*), поле идентификатор (*Identification*), поле смещение фрагмента (*fragment offset*), поле Option и поле точка дифференцированных услуг (*Differentiated Services Code Point*).

Интернет-протокол версии 6 (*IPv*6) – это усовершенствованная версия протокола *IPv*4, разработанная специально для его замены, так как последний имеет ограниченное количество адресов для выдачи всем системам в сети. *IPv*6 предполагает широкий диапазон адресов. Поскольку данный протокол имеет улучшенную безопасность, то единственным полем для вложения скрытой информации выступает поле метка потока (*Flow label*).

В работах [4] и [7] описываются принципы построения сетевой стеганографии, основанные на использовании *VoIP,* и рассматривается применение протокола *RTP* для использования скрытой передачи данных.

RTP – это протокол, используемый в аудио и видео потоках для доставки данных, в роли которых выступают пакеты в реальном времени через сеть. Данный протокол имеет способы обеспечения механизма синхронизации и управления трафиком. Полями, используемыми для техник стеганографии, являются: поле заполнение (*Padding data*), поле *Sequence number*, поле метка времени (*Timestamp*) и поле *SSRC*-идентификатор.

Существует множество программ, используемых для изменения заголовков и полезной нагрузки сетевых пакетов, а также позволяющих редактировать необязательные поля протоколов, используемые для передачи стеганограммы.

Например, программа *hping* [8] является наиболее популярной бесплатной программой для создания и изменения пакетов. С помощью программы можно формировать и отправлять собственно сформированные *TCP, UDP, ICMP* и *IP* пакеты непосредственно для применения в целях сетевой стеганографии. Данный инструмент предназначен для специалистов, так как не имеет графического интерфейса, однако является кроссплатформенным и поддерживает большое количество операционных систем, например, *Windows, MacOS, Linux, FreeBSD* и т.д.

Программа *Ostinato* [9] имеет открытый исходный код и позволяет работать с сетевыми пакетами. Данная программа также, как и *hping* поддерживает большинство популярных сетевых протоколов, позволяет генерировать сетевые пакеты и является кроссплатформенной. Программа имеет простой графический интерфейс.

Программа *Colasoft Packet Builder* [10] позволяет создавать пользовательские сетевые пакеты, умеет редактировать исходные данные в полях пакетах в формате *HEX* и декодировать их, что позволяет пользователям просто обрабатывать информацию в пакетах. Программа имеет графический интерфейс, в который входят обширные функции для работы с сетевыми данными.

Сравнение особенностей рассмотренных сетевых протоколов в рамках сокрытия информации представлено в табл. 2.

Таблица 2.

Протокол	**Уровень модели *OSI* (*TCP/IP*)**	**Особенности вложения**	**Поля пакета для вложения**	**ПО реализации**
TCP	Транспортный	Принцип гарантированной доставки без потери пакетов усложняет маневры с количеством пакета для вложения.	*Urgent pointer, Option, Sequence Number, Checksum*	*Ostinato*
UDP	Транспортный	Принцип быстрой доставки пакетов с возможными потерями позволяет маневры с их количеством и содержанием, однако понижает степень устойчивости стеганограммы и способен привести к распространению ошибок в геометрической прогрессии, тем самым увеличив вероятность раскрытия.	*Source port number, Checksum*	*Ostinato*
IPv4	Сетевой (межсетевого взаимодействия)	Определяет сетевой адрес отправителя и получателя, видоизменение которого недопустимо и легко обнаруживаемо даже в рамках локальной сети (10.0.0.0/8; 172.16.0.0/16; 192.168.0.0/24).	*Explicit Congestion Notification, Identification, Fragment offset, Option, Differentiated Services Code Point*	*Ostinato Colasoft Packet Builder*
IPv6	Сетевой (межсетевого взаимодействия)	Определяет сетевой адрес отправителя и получателя, однако в силу широкого пула адресов, допускает их изменение при условии использования динамической маршрутизации и *DHCP* сервера.	*Flow label*	*Ostinato Colasoft Packet Builder*

Протокол	Уровень модели *OSI* (*TCP/IP*)	Особенности вложения	Поля пакета для вложения	ПО реализации
RTP	Прикладной (приложений)	Имеет возможность размещения стеганоконтейнеров большого объема в силу работы с *VoIP*, однако имеет ограничения в манипуляциях со временем и числом пакетов в силу наличия механизмов обеспечения синхронизации и управления трафиком.	*Padding data, Sequence number, Timestamp, SSRC-идентификатор*	*Ostinato*
ICMP	Сетевой (межсетевого взаимодействия)	Высокая вероятность доставки в связи с тем, что межсетевые экраны и правила зачастую не блокируют данный протокол, удобен при манипуляциях с временными задержками и свободным наполнением поля данных.	*Timestamp, MTU, Data*	*Colasoft Packet Builder hping*

Заключение

Сетевая стеганография – это один из способов, предоставляющий злоумышленникам скрытый обмен информации через легитимные каналы трафика. Такой скрытый обмен информацией позволяет совершать атаки на конфиденциальные системы, закрепляясь в инфраструктуре организации и усложняя процесс выявления и обнаружения аномалий. В данной работе были рассмотрены основные методы скрытой передачи стеганограммы, способы формирования сетевых пакетов, а также инструменты, позволяющие редактировать содержимое пакетов. Понимание основных принципов и технологических методов, с помощью которой осуществляется сетевая стеганография позволяет укрепить меры защиты информации в области сетевого трафика. Поэтому развитие направления обнаружения сетевой стеганографии способствует укреплению уровня защиты сетевых инфраструктур.

Литература

1. Data Obfuscation: Steganography – ATTACK.MITRE. URL: https://attack.mitre.org/techniques/T1001/002/ (дата обращения – февраль 2024).
2. Mazurczyk W, Wendzel S., Ignacio Azagra Villares I, Szczypiorski K On importance of steganographic cost for network steganography //Security and Communication Networks, 2016. – Т. 9. – № 8. – С. 781-790.

3. Пескова О.Ю., Халабурда Г.Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи // Известия Южного федерального университета. Технические науки, 2012. – Т. 137. – № 12 (137). – С. 167-176.
4. Волкогонов В.Н., Гетьман Е.М., Салита А.С. Сокрытие информации в протоколах RTP, RTCP //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021), 2021. – С. 183-188.
5. Забиронин А.Д. Программное средство скрытой передачи информации ограниченного доступа по сетям связи общего пользования, функционирующих на основе стека протоколов TCP/IP. – Пенза, 2018. URL: https://elib.pnzgu.ru/files/eb/doc/6PRXwEekEcBg.pdf (дата обращения – февраль 2024).
6. Волкогонов В.Н., Гетьман Е.М., Салита А.С. Методы и способы создания стеганографических вложений в сетевых пакетах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021), 2021. – С. 178-183.
7. Lehner F., Mazurczyk W., Keller J., Wendzel S. Inter-protocol steganography for real-time services and its detection using traffic coloring approach // 2017 IEEE 42nd Conference on Local Computer Networks (LCN). – IEEE, 2017. – С. 78-85.
8. HPING network tool – Github. URL: https://github.com/antirez/hping (дата обращения – февраль 2024).
9. Packet/Traffic Generator and Analyzer Ostinato – Github. URL: https://github.com/pstavirs/ostinato (дата обращения – февраль 2024).
10. Packet Builder for Network Engineer – Colasoft. URL: https://www.colasoft.com/packet_builder/ (дата обращения – февраль 2024).