ЭТАЛОННАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ И ОБОСНОВАНИЕ НА ЕЕ ОСНОВЕ НОВЫХ НАПРАВЛЕНИЙ РАЗВИТИЯ ТЕОРИИ СТЕГАНОГРАФИИ

***Макаренко Сергей Иванович**, кандидат технических наук*

В работе уточняется и дополняется терминологический базис теории стеганографии, а также предлагается обобщение известных методов и способов реализации стеганографических систем связи на основе эталонной модели взаимодействия стеганографических систем. Данная модель формализует описание взаимодействия абонентов стеганографических систем связи на различных функциональных уровнях: уровне системы связи, уровне контейнера, уровне стегоканала, уровне стегосети, уровне стеготранспорта, уровне сообщений. Представлены объекты, предметы и процессы, формализуемые на каждом из уровней. Приводятся перспективные направления развития стеганографических систем связи на основе предложенной модели.

***Ключевые слова**: стеганография, скрытая передача данных, стеганографическая система.*

THE STEGANOGRAPHIC SYSTEM INTERCONNECTION BASIC REFERENCE MODEL AND THE JUSTIFICATION OF NEW AREAS OF STEGANOGRAPHY THEORY'S DEVELOPMENT

***Sergey Makarenko**, Ph.D. in Technical Sciences*

This article consists of revision terms of steganography theory and suggest the steganographic system interconnection basic reference model (SSI model) for generalization of researched steganography methods and means. This model formalizes the interconnection of steganographic communication systems` users on different function levels: communication level, steganography container level, steganography channel level, steganography network level, steganography transport level and message level. Objects, subjects and process of steganography systems define for every this levels. The perspective areas of development of steganographic communication systems based on SSI model are shown.

***Keywords**: steganography, undetected data communications, steganographic systems.*

Глобальное распространение вычислительных и телекоммуникационных систем привело к необходимости обеспечения безопасности передаваемых данных, доступа к ним, а также защиты авторских прав на различные виды информации, циркулирующей в интернете. В связи с этим, стеганография как теория скрытия информации получила новый импульс к развитию. В настоящее время методы стеганографии условно делят на:

– классическую стеганографию — включает в себя «некомпьютерные методы»;

– компьютерная стеганографию — направление классической стеганографии, основанное на реализации методов стеганографии на основе вычислительных и телекоммуникационных платформ и использования специальных свойств обрабатываемых и передаваемых форматов данных;

– цифровую стеганографию — направление компьютерной стеганографии, основанное на сокрытии информации в цифровых объектах, изначально имеющих аналоговую природу (изображения, видео, звуки).

В работах [1-3] показано, что к основным направлениям приложения современной теории

компьютерной стеганографии относятся следующие:

– организация стеганографических (скрытых) систем связи на основе современных телекоммуникационных систем и противодействие им;

– обеспечение целостности и подлинности информационных ресурсов за счет встраивания цифровых водяных знаков;

– обеспечение целостности и идентификации информационных ресурсов за счет встраивания идентификационных номеров;

– дополнение информационных ресурсов за счет встраивания в них заголовков.

Однако анализ основных монографий [1-3], некоторых публикаций [4-6], а также диссертационных исследований [7-17] в предметной области компьютерной стеганографии показал, что ее современная теория обладает рядом недостатков, позволяющих обосновать новые направления ее дальнейшего развития:

– не устоявшийся и неоднозначный терминологический базис;

– глубокая проработанность теоретических основ создания стегосистем и недостаточное исследование аспектов проведения атак на стеганографические системы;

– широкое освещение теоретических вопросов, посвященных цифровым водяным знакам, при недостаточной проработанности теории построения стеганографических систем связи с использованием имеющегося задела в теории передачи информации, теории систем связи, теории информационной безопасности.

В данной статье предлагается эталонная модель, направленная на устранение последнего из вышеуказанных недостатков, которая может быть использована как для формализованного описания уже известных стеганографических систем, так и для создания принципиально новых решений в данной области, часть которых представлена ниже.

В теории систем связи основой формализованного описания взаимодействия абонентов составляет эталонная модель взаимодействия открытых систем (OSI – open systems interconnection) [18]. Декомпозиция информационного обмена абонентов посредством систем связи на уровни позволило формализовать различные аспекты взаимодействия абонентов, разделяя их в соответствии с функционалом решаемых задач. Предлагается перенести подход к декомпозиции взаимодействия абонентов на различные уровни, используемый в модели OSI, на взаимодействие абонентов стеганографической системы связи, с учетом особенностей последней.

Для описания взаимодействия абонентов стеганографической системы связи в рамках предлагаемой эталонной модели предлагается определиться с терминологическим базисом в рамках которого будет вестись описание модели.

На основе известного понятийного аппарата теории передачи информации, теории систем связи, теории информационной безопасности предлагается уточнить семантическую область ряда применяемых в теории стеганографии терминов (выделены курсивом), а также ввести новые понятия, ранее в этой области не используемые.

Сообщение – скрытно передаваемая информация.

Контейнер (стегоконтейнер) – информация, в которую встраивается тайное сообщение. Пустой контейнер – контейнер, не содержащий скрытого сообщения. Заполненный контейнер (стегоконтейнер) – контейнер, содержащий скрытое сообщение.

Стегоключ - секретный ключ, используемый для сокрытия сообщения в стегоконтейнере.

Стеганографическая связь (стегосвязь) – скрытый обмен сообщениями за счет их встраивания в другую информацию, передаваемую по системе связи.

Вид стегосвязи – классификационная группа стегосвязи, выделяемая по виду предаваемого сообщения (данные, текст, голос, видео, изображение и др.).

Род стегосвязи – классификационная группа стегосвязи, выделяемая по виду контейнера в который страивается сообщения (данные, текст, голос, видео, изображение и др.).

Абонент системы стеганографической связи – отправитель или получатель скрытых сообщений.

Стеганографическая система связи (стегосистема) – совокупность взаимоувязанных и согласованных по задачам, месту и времени методов и средств, стегоузлов и стегоканалов функционирующих в интересах обслуживания абонентов, ведущих скрытый обмен сообщениями.

Узел стеганографической связи (стегоузел) – элемент стегосистемы, представляющий собой объединение методов и средств для образования стегоканалов, их распределении и коммутации, извлечения и встраивания сообщений, передаваемых по стегоканалам различного рода, а также предоставление абонентам стегосистемы услуг по скрытому обмену сообщениями.

Канал стеганографической связи (стегоканал) – объединение методов и средств (стегокодер, стегодетектор, стегодекодер), используемых для создания определенного рода стегосвязи

между стегоузлами. В традиционных работах по стеганографии раннее данному определению соответствовало понятие стегосистемы.

Стегокодер – устройство, предназначенное для осуществления вложения скрытого сообщения в контейнер.

Стегодетектор – устройство, предназначенное для определения наличия сообщения в контейнере.

Стегодекодер – устройство, восстанавливающее скрытое сообщение из контейнера.

Сеть стеганографической связи (стегосеть) – совокупность узлов стегосистемы и соединяющих их стегоканалов.

Направление стеганографической связи (стегонаправление) – совокупность стегоканалов и стегоузлов, обеспечивающих стегосвязь между двумя абонентами.

Система управления стеганографической связью – часть стегосистемы, обеспечивающая функционирование ее с заданным качеством.

Качество стеганографической связи – свойство стегосвязи, по обеспечению своевременной и достоверной передаче сообщений.

Своевременность стеганографической связи – способность стегосвязи обеспечивать передачу сообщений по стегосистеме в заданное время.

Достоверность стеганографической связи – способность стегосвязи обеспечивать воспроизведение передаваемых сообщений в пунктах приема с заданной точностью.

Готовность элемента стегосистемы – состояние элемента стегосистемы, характеризующее степень его готовности к выполнению своих функций по обеспечению стегосвязи.

Пропускная способность стегосистемы – максимальное количество сообщений (информации), которое с заданным качеством может передать стегосистема за единицу времени.

Стегоанализ – процесс определения факта наличия стегосвязи и параметров стегосистемы.

Атака на стегосистему – активные или пассивные действия противника/нарушителя по стегоанализу, нарушению корректного функционирования стегосистемы, уничтожению, искажению либо подмене передаваемых по ней сообщений.

Стеганографическая стойкость (стегостойкость) – свойство, определяющее способность стегоконтейнера и скрытого в нем сообщения противостоять возможным атакам на них. Стеганографическую стойкость традиционно рассматривают в трех аспектах, соответствующих передаче сообщений в контейнере:

- невозможность определения факта нахождения скрытого сообщения в стегоконтейнере (скрытность сообщения);

- невозможность извлечения данных из стегоконтейнера, при определении факта наличия стегоконтейнера;

- невозможность прочтения сообщения после извлечения данных из стегоконтейнера.

Стеганографическая скрытность (стегоскрытность) – свойство стегосистемы и ее отдельных элементов, по способности обеспечивать невозможность определения факта ведения стегосвязи. Предлагается отличать стегоскрытность от стегостойкости, так как понятие стегоскрытности характеризует свойство скрытности применительно не к стегоконтейнеру, а к таким объектам как стегоканал, стегосеть, стегосистема.

Устойчивость стегосистемы (стегоустойчивость) – свойство, определяющее способность стегосистемы и ее отдельных элементов обеспечить заданное качество стегосвязи в условиях воздействия различных деструктивных факторов и атак на нее. Предлагается различать свойство устойчивости (отличительным признаком которой является наличие условий воздействия различных деструктивных факторов и атак, направленных на нарушение функционирования стегосистемы), от свойства скрытности (отличительным признаком которой является условия проведения атак направленных на выявление факта стегосвязи) .

Устойчивость сообщения – свойство сообщения, определяющее возможность его воспроизведения в пунктах приема с заданным уровнем достоверности, в условиях преобразования и изменения параметров контейнера.

Имитостойкость стегосистемы – способность стегосистемы противостоять вводу в нее ложных, в том числе и ранее переданных, сообщений, а также навязыванию ей ложных режимов работы.

Взаимосвязь представленных понятий для объектов стегосистемы, свойств стегосистемы и стегосвязи, а также для характерных в данной предметной области деструктивных воздействий предст авлено на рис. 1.

На основе этих понятий предлагается формализовать взаимодействие абонентов стеганографической системы связи в виде многоуровневой **эталонной модели взаимодействия стеганографических систем - ЭМВСС (Steganographically Systems Interconnection basic reference model – SSI model).** Данная эталонная модель позволяет обобщить имеющиеся работы в области стеганографического сокрытия сообщений в контейнерах [1-15, 19] и органично развить направления работ [8, 16, 17, 20-22] в направлении создания единой формализованной модели стегосистемы, как одного из вариантов реализации системы

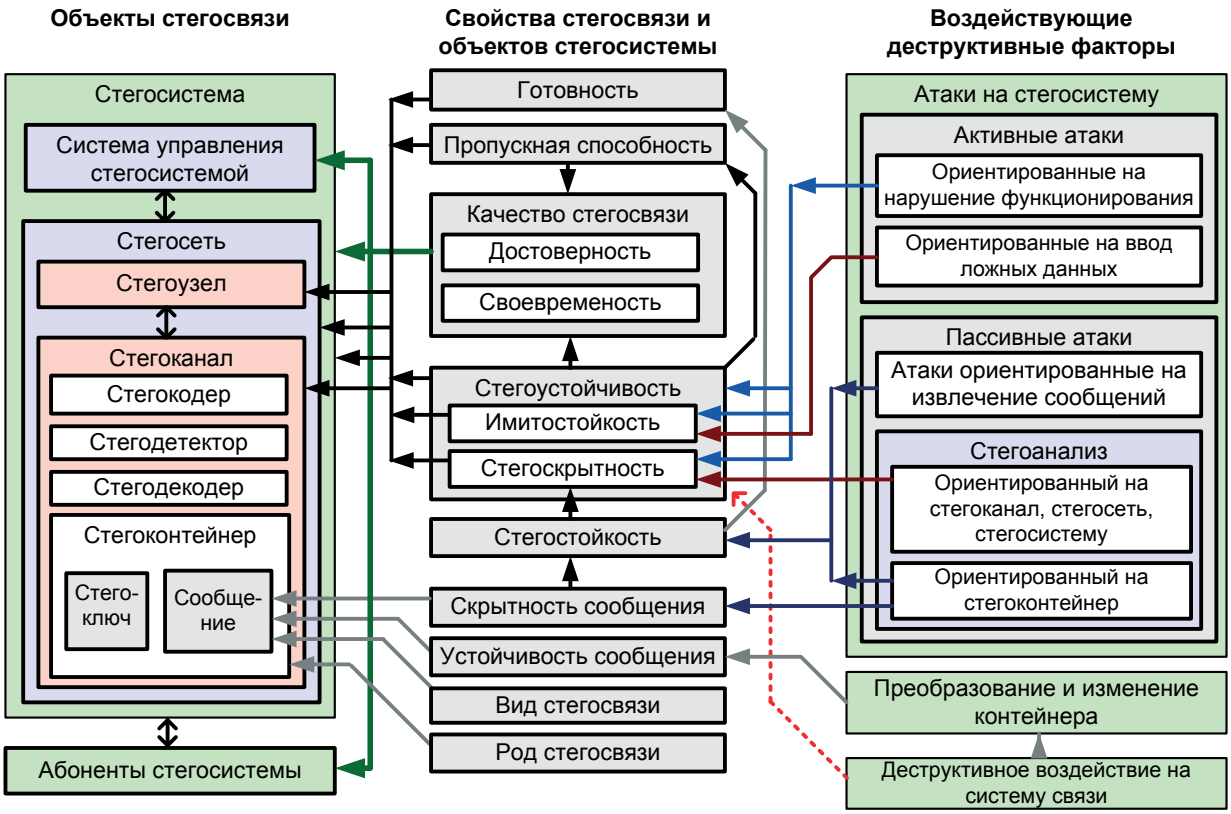

***Рис. 1**. Взаимосвязь представленных определений объектов стегосистемы, свойств стегосистемы и стегосвязи, а также характерных для данной предметной области деструктивных воздействий*

скрытой передачи сообщений, наложенной на телекоммуникационную систему связи.

На первом уровне ЭМВСС (уровень системы связи) рассматривается система связи, реализующая информационный обмен контейнерами. Этот уровень описывается в соответствии с семиуровневой моделью OSI [18]. Также на данном уровне предлагается формализовать модели доступа к системе связи и воздействия на нее нарушителя/противника в соответствии со стандартными моделями информационной безопасности [23].

На втором уровне ЭМВСС (уровень стегоконтейнера) предлагается формализовать процессы, связанные с встраиванием и извлечением сообщения в контейнер, процессы формирования и управления ключевой информацией на уровне отдельных контейнеров. Здесь же предлагается формализовать вопросы устойчивости сообщений к преобразованию контейнера, а также учитывать различные рода стегосвязи. На данном уровне предлагается описать методы стегоанализа, направленные на вскрытие факта нахождения сообщения в контейнере, а также атаки (как активные, так и пассивные) направленные на контейнер и передаваемое в нем сообщение. Отдельные показатели и критерии, описывающие свойства и эффективность формализуемых на данном уровне процессов, в частности понятие стеганографической стойкости, тоже соответствует данному уровню модели ЭМВСС.

Проведенный анализ работ по теории стеганографии показал, что подавляющее их количество соответствует формализации процессов на уровне стегоконтейнера и рассматривает различные аспекты встраивания сообщений в видео- [1, 19], аудио- [1-3, 7, 9], графические данные [1-3, 9-12, 14, 15], текст [3], а так же в различные служебные поля и заголовки пакетов систем связи [1-3, 8, 13]. Работы по стегоанализу и атакам, направленным на контейнеры различного рода [1-3, 4-6], также могут быть отнесены к данному уровню.

На третьем уровне ЭМВСС (уровень стегоканала) предлагается формализовать процессы, связанные с образованием стегоканалов различных родов; процессы стегокодирования, стегодетектирования, стегодекодирования в стегоканале; управления в стегоканалах ключевой информацией для отдельных контейнеров (соответственно - объемом и стеганографической стойкостью сообщений); разделения стегоканала и множественного доступа абонентов к нему, а также параметры отдельного стегоканала: скрытность, пропускная способность, своевременность, устойчивость. На этом уровне предлагается описать задачи стегоа-

нализа по выявлению факта наличия стегоканала, а также атаки направленные на стегоканал.

Анализ опубликованных работ показал, что в большинстве исследований рассматривается моно-стегоканал, без учета возможности его разделения между абонентами, или предоставления к нему множественного доступа. В частности, среди открытых работ только в работах [19, 22] рассматривается вариант кодового множественного доступа к стегоканалу [19] и пространственно-временное разделение стегоканала [22]. При этом основной характеристикой стегоканала считают пропускную способность [1, 3], без учета характеристик его своевременности и устойчивости. Также в имеющихся работах присутствует путаница с применением понятия «стеганографической стойкости». В связи с этим понятие «стеганографическая стойкость» в том контексте в котором она рассматривается в работах [1-5] предлагается целиком отнести к уровню стегоконтейнера, а на уровне стегоканала оперировать понятиями устойчивости и скрытности стегоканала, определение которых предложено в данной работе.

На четвертом уровне ЭМВСС (уровень стегосети) предлагается ввести новые понятия стегосети и стегоузла и формализовать процессы, соответствующие скрытому обмену сообщениями по множеству стегоканалов, входящих в стегосеть, а также процессы преобразования сообщений в стегоузлах. К процессам, формализуемым на

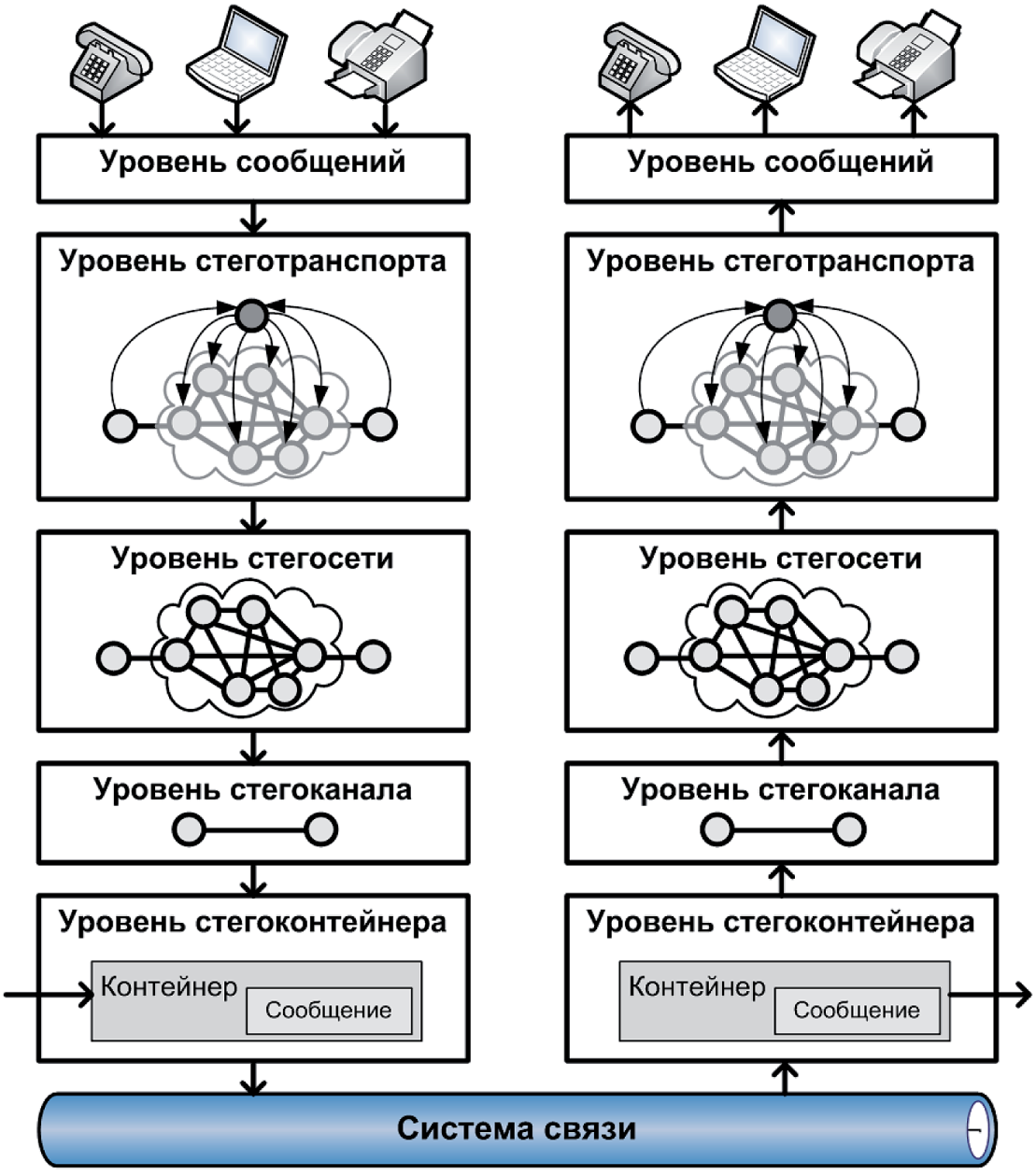

Рис. 2. *Структура взаимодействия уровней ЭМВСС*

Таблица. *Предложения по формализации объектов, предметов и различных аспектов взаимодействия абонентов стеганографической системы на уровнях ЭМВСС*

№	Уровни модели	Объекты и предметы стеганографической системы
1	Уровень системы связи	**Объекты уровня** Система связи, реализующая передачу стегоконтейнера. Противник/нарушитель. **Предметы уровня** Методы обеспечения заданного качества функционирования системы связи в соответствии с моделью OSI.
2	Уровень стегоконтейнера	**Объекты уровня стегоконтейнера** Стегоконтейнер. Сообщение. **Предметы уровня стегоконтейнера** Метод встраивания сообщений в стегоконтейнер. Методы формирования ключевой информации. Методы обеспечения заданного уровня устойчивости сообщений в условиях преобразования и изменения параметров контейнера. Методы обеспечения стегонаграфической стойкости и ее аспекты на уровне стегоконтейнера. Методы стегоанализа контейнера. Методы проведения атак на стегоконтейнер.
3	Уровень стегоканала	**Объекты уровня** Стегоканал. Параметры стегоканала: скрытность, пропускная способность, своевременность, устойчивость. Абоненты стегоканала. **Предметы уровня** Методы множественного доступа абонентов к стегоканалу. Методы управления ключевой информацией контейнеров. Методы стегоанализа стегоканала. Методы проведения атак на стегоканал.
4	Уровень стегосети	**Объекты уровня** *Стегосеть.* *Абоненты, узлы и стегоканалы стегосети.* **Предметы уровня** *Методы объединения стегоканалов в стегосеть.* *Методы управления параметрами и ключевой информацией стегоканалов.* *Методы маршрутизации сообщений в стегоузлах по стегоканалам.* *Методы преобразования сообщений в узлах сетгосети.* *Методы оценки, измерения и контроля параметров стегоканалов в стегосети.* *Методы обеспечения устойчивости и скрытности потоков сообщений в стегосетях.* *Методы стегоанализа стегосетей.* *Методы проведения атак на стегосети.*
5	Уровень стеготранспорта	**Объекты уровня** *Абоненты стеганографической системы связи.* *Информационные направления стегосвязи.* **Предметы уровня** *Методы обеспечения заданной своевременности, пропускной способности, устойчивости, скрытности при передачи сообщений по стегонаправлениям связи.* *Методы управления ресурсами и параметрами стегосети для обеспечения заданного качества обслуживания при передаче сообщений.*
6	Уровень сообщений	**Объекты уровня** *Виды информации представляемые к передаче в виде сообщений.* **Предметы уровня** *Требования по качеству обслуживания информации передаваемой в виде сообщений.* *Методы разборки/сборки сообщений конечными абонентами.* *Методы борьбы с ошибками потери или дублирования сообщений с учетом вида передаваемой информации.*

данном уровне, целесообразно отнести: объединение отдельных стегоканалов в стегосеть, маршрутизацию сообщений по стегоканалам, преобразование сообщений в стегоузлах. На данном уровне п редлагается формализовать: методы оценки, измерения и контроля параметров отдельных стегоканалов в стегосети; методы управления параметрами и ключевой информацией отдельных стегоканалов; методы обеспечения устойчивости и скрытности потоков сообщений в стегосетях. Модели противника/нарушителя, методы стегоанализа и проведения атак, ориентированных на стегосети в целом, также стоит отнести к данному уровню.

На пятом уровне ЭМВСС (уровень стеготранспорта) предлагается ввести новое понятие «направление стегосвязи» как совокупности стегоканалов и стегоузлов обеспечивающих стегосвязь между двумя абонентами и отнести к данному уровню: вопросы управления ресурсами и параметрами стегосети и отдельных стегоканалов для обеспечения заданного качества обслуживания сообщений; методы и средства обеспечения заданной своевременности, пропускной способности, устойчивости и скрытности при передаче сообщений по направлениям стегосвязи, в том числе в условиях стегоанализа и атак нарушителя. При формализации и классификации решаемых задач управления ресурсами стегосети предлагается взять за основу концепцию управления TMN (Telecommunication Management Network), в дальнейшем модифицировав ее с учетом особенностей стегосвязи.

На шестом уровне ЭМВСС (уровень сообщений) предлагается рассмотреть: требования конечных абонентов сети к качеству обслуживания передаваемых ими сообщений; виды информации (данные, голос, видео, изображения) представляемые к встраиванию в виде сообщений; требования к параметрам и качеству обслуживания сообщений, содержащих соответствующий вид информации, в том числе и особенности разборки/сборки сообщений передаваемой информации абонентами стегосистемы. Предполагается, что требования к качеству обслуживания сообщений являются входными ограничениями для методов управления рассматриваемых на уровне стеготранспорта.

В настоящее время работы, соответствующие процессам, формализованным в рамках предлагаемой модели ЭМВСС на уровнях стегосети, стеготранспотра и стегосообщений, автору неизвестны.

Предложения по уровням модели ЭМВСС и формализации объектов, предметов и различных аспектов взаимодействия абонентов стеганографической системы связи на данных уровнях представлены на рис. 2. и в таблице.

В таблице, ранее отсутствующие элементы научно-методического аппарата описания взаимодействия стеганографических систем выделены курсивом.

Перенос в модель ЭМВСС части функциональных особенностей из модели OSI позволил:

– обобщить в формализованном виде существующие теоретические основы построения, функционирования и анализа стеганографических систем;

– предложить новые направления развития стеганографических систем, на основе которых могут быть обоснованы принципиально новые прикладные решения.

В частности, к новым направлениям прикладного развития стеганографических систем связи, которые могут быть основаны на вышеприведенной модели, можно отнести:

– существенное увеличение пропускной способности направлений стегосвязи за счет использования многоканальной передачи сообщений, с одновременным повышением скрытности отдельных стегоканалов, за счет уменьшения объема сообщений, передаваемых по каждому конкретному стегоканалу;

– передача голосовой, видео и графической информации при разборке их на сообщения с учетом вида информации, и последующей их передачей с обеспечением качества обслуживания сообщений в направлениях стегосвязи с заданной пропускной способностью;

– построение распределенных в информационном пространстве стеганографических систем связи в которых обеспечение заданного уровня устойчивости и скрытности обеспечивается значительным наращиванием связности топологии стегосетей и направлений стегосвязи, с одновременным снижением пропускной способности отдельных стегоканалов, и обьема встраиваемых сообщений;

– построение адаптивных к действиям нарушителя/противника стегосистем за счет реализации новых методов и способов управления ресурсами стегосистем и ключевой информацией в них;

– разработка новых способов стегоанализа, направленных на вскрытие факта существования, а также противодействие стегосетям и направлениям стегосвязи.

Таким образом, предложенная модель ЭМВССС может быть использована не только для обобщения и развития теории стеганографичесих систем, но может быть положена в основу принципиаль-

но новых алгоритмических, программных и технических решений по созданию стегосистем.

Предложенная в работе терминология и обобщенная модель ЭМВСС не являются окончательными, носят дискуссионный характер и автор надеется, что они найдут свое дальнейшее развитие и будут востребованы специалистами в области стеганографии.

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2009. 272 с.
2. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стегоанализ. Монография. М.: Вузовская книга, 2009. 220 с.
3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
4. Разинков Е.В., Латыпов Р.Х. Стойкость стегонографических систем // Ученые записки Казанского гос. ун.-та. Физ.-мат. науки. 2009. Т. 151. Кн. 2. С. 126-132.
5. Ремизов А.В., Филиппов М.В. Оценка необнаружимости стеганографических алгоритмов // Наука и образование. 2012. № 3. URL: http://technomag.edu.ru/doc/359383.html (дата доступа 17.04.2014)
6. Сизов А.С., Никутин Е.И., Котенко С.В. Обзор и тенденции развития методов анализа стеганографических систем // Известия Юго-Западного государственного университета. Серия Управление, вычислительная техника, информатика. Медицинское приборостроение. 2013. № 4. С. 43-48.
7. Аленин А.А. Разработка и исследование методов скрытой передачи информации в аудиофайлах. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.15. Самара: ПГУТИ, 2011. 174 с.
8. Алиев А.Т. Разработка моделей, методов и алгоритмов перспективных средств защиты информации в системах электронного документооборота на базе современных технологий скрытой связи. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. Ростов-на-Дону: ЮФУ, 2008. 216 с.
9. Дрюченко М.А. Статистические и нейросетевые алгоритмы синтеза и анализа стеганографически скрытой информации в аудио- и графических данных. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.17. Воронеж: ВГУ, 2010. 192 с.
10. Жилкин М.Ю. Теоретико-информационные методы стегоанализа графических данных. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.12.13. Новосибирск: СибГУТИ, 2009. 153 с.
11. Кувшинов С.С. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. СПб.: НИУ ИТМО, 2010. 116 с.
12. Мерзлякова Е.Ю. Построение стеганографических систем для растровых изображений, базирующихся на теоретико-информационных принципах. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. Новосибирск: СибГУТИ, 2011. 161 с.
13. Пономарев К.И. Некоторые математические модели стеганографии и их статистический анализ. Дисс. на соиск. уч. ст. канд. ф.-мат. наук по спец. 01.01.05. М.: МИЭМ, 2010. 81 с.
14. Разинков Е.В. Математическое моделирование стеганографических объектов и методы вычисления оптимальных параметров стегосистем. Дисс. на соиск. уч. ст. канд. ф.-мат. наук по спец. 05.13.18. Казань: КГУ, 2012. 109 с.
15. Рублев Д.П. Разработка и исследование высокочувствительных методов стегоанализа. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. Таганрог: ТТИ ЮФУ, 2007. 139 с.
16. Жгун А.В. Модель скрытой передачи информации в каналах связи Дисс. на соиск. уч. ст. канд. ф.-мат. наук по спец. 05.13.18. В. Новгород: НовГУ, 2003. 187 с.
17. Жгун А.А. Модель скрытой передачи информации для дискретных каналов с повышенным уровнем помех. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.18. В. Новгород: НовГУ, 2010. – 216 с.
18. Макаренко С.И. Вычислительные системы, сети и телекоммуникации: учебное пособие. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2008. 352 с.
19. Абазина Е.С. Формирование стеганографического канала с кодовым уплотнением на основе двумерных нелинейных сигналов // Вопросы радиоэлектроники в сфере техники телевидения. 2014. № 1. С. 73-81.
20. Орлов В.В. Методы скрытой передачи информации в телекоммуникационных сетях. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.12.13. Самара: ПГУТИ, 2012. 166 с.
21. Макаров М.И. Разработка и исследование методов скрытой распределенной передачи сеансовых данных в телекоммуникационных сетях. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.12.13. Самара: ПГУТИ, 2013. 144 с.
22. Алексеев А.П., Макаров М.И. Принципы многоуровневой защиты информации // Инфокоммуникационные технологии. 2012. Т. 10. № 2. С. 88-93.
23. Макаренко С.И. Информационная безопасность: учебное пособие для студентов вузов. Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. 372 с.

Reference

1. Gribunin V.G., Okov I.N., Turincev I.V. Cifrovaja steganografija. M.: Solon-Press, 2009. 272 s. [Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography. Moscow: Solon-Press, 2009. 272 p. (In Russia)]
2. Agranovskij A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. Steganografija, cifrovye vodjanye znaki i stegoanaliz. Monografija. M.: Vuzovskaja kniga, 2009. 220 s. [Agranovskij A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. Steganography, digital water marks and steganoanalysis. Treatise. Moscow: Vuzovskaja kniga, 2009. 220 p. (In Russia)]
3. Konahovich G.F., Puzyrenko A.Ju. Komp'juternaja steganografija. Teorija i praktika. K.: MK-Press, 2006. 288 s. [Konahovich G.F., Puzyrenko A.Ju. Computer-held steganography. Theory and practice. Kiev: MK-Press, 2006. 288 p. (In Russia)]
4. Razinkov E.V., Latypov R.H. Stojkost' stegonograficheskih system // Uchenye zapiski Kazanskogo Universiteta. Seria Fiziko-Matematicheskie Nauki. 2009. T. 151. Kn. 2. S. 126-132. [Razinkov E.V., Latypov R.H. The constancy of steganographic systems // Uchenye zapiski Kazanskogo Universiteta. Seria Fiziko-Matematicheskie Nauki. 2009. Vol. 151/2. pp. 126-132. (In Russia)]
5. Remizov A.V., Filippov M.V. Ocenka neobnaruzhimosti steganograficheskih algoritmov // Nauka i obrazovanie. 2012. № 3. URL: http://technomag.edu.ru/doc/359383.html (data dostupa 17.04.2014) [Remizov A.V., Filippov M.V. The rating of nondetectable

steganographic algorithms // Nauka i obrazovanie. 2012. № 3. URL: http://technomag.edu.ru/doc/359383.html]
6. Sizov A.S., Nikutin E.I., Kotenko S.V. Obzor i tendencii razvitija metodov analiza steganograficheskih sistem // Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta. Serija Upravlenie, vychislitel'naja tehnika, informatika. Medicinskoe priborostroenie. 2013. № 4. S. 43-48. [Sizov A.S., Nikutin E.I., Kotenko S.V. Overview and trends of the analysis methods of steganographic messages development // Proceedings of the southwest state university. 2013. № 4. pp. 43-48. (In Russia)]
7. Alenin A.A. Razrabotka i issledovanie metodov skrytoj peredachi informacii v audiofajlah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.15. Samara: PGUTI, 2011. 174 s. [Alenin A.A. The development and analysis of nondetectable data communication in audio files` methods. Diss. Ph.D. Samara: Povolzhskiy State University of Telecommunications and Informatics, 2011. 174 p. (In Russia)]
8. Aliev A.T. Razrabotka modelej, metodov i algoritmov perspektivnyh sredstv zashhity informacii v sistemah jelektronnogo dokumentooborota na baze sovremennyh tehnologij skrytoj svjazi. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19 Rostov-na-Donu: JuFU, 2008. 216 s. [Aliev A.T. The development of models, methods and algorithms of perspective data protection means in electronic document management systems, based on present-day technologies of nondetectable data communication. Diss. Ph.D. Rostov-na-Donu: South Federal University, 2008. 216 p. (In Russia)].
9. Drjuchenko M.A. Statisticheskie i nejrosetevye algoritmy sinteza i analiza steganograficheski skrytoj informacii v audio- i graficheskih dannyh. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.17. Voronezh: VGU, 2010. 192 s. [Drjuchenko M.A. Statistical and neuronet algorithms of synthesis and analysis of steganographically nondetectable data in audio and graphic files. Diss. Ph.D. Voronezh: Voronezh State University, 2010. 192 p. (In Russia)]
10. Zhilkin M.Ju. Teoretiko-informacionnye metody stegoanaliza graficheskih dannyh. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.12.13. Novosibirsk: SibGUTI, 2009. 153 s. [Zhilkin M.Ju. Information-theoretical methods of steganoanalysis of graphic data. Diss. Ph.D. Novosibirsk: Siberian State University of Telecommunications and Information Sciences, 2009. 153 p. (In Russia)]
11. Kuvshinov S.S. Metody i algoritmy sokrytija bol'shih ob'emov dannyh na osnove steganografii. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19. SPb.: NIU ITMO, 2010. 116 s. [Kuvshinov S.S. Methods and algorithms of big data` hiding based on steganography. Diss. Ph.D. St. Petersburg: Saint-Petersburg National Research University of Information technologies, mechanics and Optics, 2010. 116 p. (In Russia)]
12. Merzljakova E.Ju. Postroenie steganograficheskih sistem dlja rastrovyh izobrazhenij, bazirujushhihsja na teoretiko-informacionnyh principah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19. Novosibirsk: SibGUTI, 2011. 161 s. [Merzljakova E.Ju. Steganographic systems` development for bit-map images, based on –theoretic-informational concepts. Diss. Ph.D. Novosibirsk: Siberian State University of Telecommunications and Information Sciences, 2011. 161 p. (In Russia)]
13. Ponomarev K.I. Nekotorye matematicheskie modeli steganografii i ih statisticheskij analiz. Diss. na soisk. uch. st. kand. f.-mat. nauk po spec. 01.01.05. M.: MIJeM, 2010. 81 s. [Ponomarev K.I. Some mathematical../../../../../../user/AppData/Local/Temp/1406428456 models of steganography and statistical analysis of them. Diss. Ph.D. Moscow: Moscow Institute of Economics and Mathematics. 2010. 81 p. (In Russia)]
14. Razinkov E.V. Matematicheskoe modelirovanie steganograficheskih ob'ektov i metody vychislenija optimal'nyh parametrov stegosistem. Diss. na soisk. uch. st. kand. f.-mat. nauk po spec. 05.13.18. Kazan': KGU, 2012. 109 s. [Razinkov E.V. The mathematical modeling of steganographic objects and methods of optimal parameters of steganographic systems` calculation. Diss. Ph.D. Kazan: Kazan State University, 2012. 109 p. (In Russia)]
15. Rublev D.P. Razrabotka i issledovanie vysokochuvstvitel'nyh metodov stegoanaliza. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19. Taganrog: TTI JuFU, 2007. 139 s. [Rublev D.P. The development and analysis of highly sensitive methods of steganoanalysis. Diss. Ph.D. Taganrog: Taganrog Institute of Radio Engineering, 2007. 139 p. (In Russia)]
16. Zhgun A.V. Model' skrytoj peredachi informacii v kanalah svjazi Diss. na soisk. uch. st. kand. f.-mat. nauk po spec. 05.13.18. V. Novgorod: NovGU, 2003. 187 s. [Zhgun A.V. The model of nondetectable data communication. Diss. Ph.D. Gteat Novgorod: Novgorod State University, 2003. 187 p. (In Russia)]
17. Zhgun A.A. Model' skrytoj peredachi informacii dlja diskretnyh kanalov s povyshennym urovnem pomeh. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.18. V. Novgorod: NovGU, 2010. 216 s. [Zhgun A.V. The model of nondetectable data communication for the channels with raised level of noise. Diss. Ph.D. Gteat Novgorod: Novgorod State University, 2010. 216 p. (In Russia)]
18. Makarenko S.I. Vychislitel'nye sistemy, seti i telekommunikacii: uchebnoe posobie. Stavropol': SF MGGU im. M. A. Sholohova, 2008. 352 s. [Makarenko S.I. Computer systems, networks and telecommunication: Tutorial. Stavropol: Sholokhov Moscow State University for the Humanities (Stavropol branch), 2008. 352 p. (In Russia)]
19. Abazina E.S. Formirovanie steganograficheskogo kanala s kodovym uplotneniem na osnove dvumernyh nelinejnyh signalov // Voprosy radiojelektroniki. Seria: tehnika televidenija. 2014. № 1. S. 73-81. [Abazina E.S. Forming of stenography data link with code consolidation based on two-dimensional nonlinear signals // Voprosy radiojelektroniki. Seria: tehnika televidenija. 2014. № 1. pp. 73-81.]
20. Orlov V.V. Metody skrytoj peredachi informacii v telekommunikacionnyh setjah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.12.13. Samara: PGUTI, 2012. 166 s. [Orlov V.V. Methods of nondetectable data communication in telecommunication networks. Diss. Ph.D. Samara: Povolzhskiy State University of Telecommunications and Informatics, 2012. 166 p. (In Russia)]
21. Makarov M.I. Razrabotka i issledovanie metodov skrytoj raspredelennoj peredachi seansovyh dannyh v telekommunikacionnyh setjah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.12.13. Samara: PGUTI, 2013. 144 s. [The development and analysis of methods of nondetectable allocated session data in telecommunication networks. Diss. Ph.D. Samara: Povolzhskiy State University of Telecommunications and Informatics, 2013. 144 p. (In Russia)]
22. Alekseev A.P., Makarov M.I. Principy mnogourovnevoj zashhity informacii // Infokommunikacionnye tehnologii. 2012. T. 10. № 2. S. 88-93. [Alekseev A.P., Makarov M.I. Principles of multilevel protection of the information // Infokommunikacionnye tehnologii. 2012. Vol. 10. № 2. pp. 88-93. (In Russia)]
23. Makarenko S.I. Informacionnaja bezopasnost': uchebnoe posobie dlja studentov vuzov. Stavropol': SF MGGU im. M.A. Sholohova, 2009. 372 s. [Makarenko S.I. Information security: Tutorial. Stavropol: Sholokhov Moscow State University for the Humanities (Stavropol Branch), 2009. 372 p. (In Russia)]