DOI: 10.15514/ISPRAS–2020–32(6)–9

Способ маскирования передаваемой информации

[1] *П.В. Закалкин, ORCID: 0000-0003-2946-2586 <pzakalkin@mail.ru>*
[1] *С.А. Иванов, ORCID: 0000-0002-0528-276X <sa-ivanov@inbox.ru>*
[1] *Е.В. Вершенник, ORCID: 0000-0003-3647-741X <sukhorukova_lena@mail.ru>*
[2] *А.В. Кирьянов, ORCID: 0000-0001-6104-7433 <alex1175@mail.ru>*

[1] *Военная академия связи им. С.М. Буденного,*
194064, Россия, Санкт-Петербург, Тихорецкий проспект, д. 3
[2] *Академия Федеральной Службы охраны Российской Федерации,*
302015, Россия, г. Орел, ул. Приборостроительная, д. 35

Аннотация. Процессы глобализации, появление и активное развитие киберпространства привели к необходимости защиты информации, передаваемой в рамках информационного обмена. Существующие подходы к защите информации, а в частности ее шифрование, стеганография и т.п. с точки зрения информационного обмена имеют ряд демаскирующих признаков, которые, при всей несомненной надежности этих подходов, существенно снижают скрытность передачи информации. Предлагаемая статья рассматривает подход, позволяющий осуществлять скрытую передачу защищаемой информации по открытым каналам связи, за счет маскирования передаваемой информации. Разработка предлагаемого подхода осуществлялась поэтапно, на первом этапе был разработан и запатентован способ маскирования передаваемой информации. На следующем этапе, на основе разработанного способа, создана функциональная модель клиентского и серверного приложений комплекса передачи скрытой информации. Передачу маскированной информации предлагается осуществлять с помощью разработанного протокола скрытой передачи информации. Структурная схема пакета предлагаемого протокола передачи скрытой информации, вариант реализации и использования протокола на прикладном уровне представлены в работе. На заключительном этапе, разработана программная реализация предлагаемого подхода и осуществлено моделирование информационного обмена при различном окне смещения. В работе представлена функциональная модель разработанного комплекса, схема взаимодействия функциональных модулей, и блок-схема предлагаемого подхода к маскированию передаваемой информации. Повышение скрытности передачи информации обеспечивается за счет процедуры преобразования несущего сообщения в маркерное путем формирования окна смещения, а также использования массива цифровых записей для выбора несущего сообщения. Предлагаемый подход позволяет при увеличении размера окна и использовании скользящего окна использовать меньшее несущее сообщение, в зависимости от размера информационного сообщения выбирать оптимальный размер несущего сообщения и окна смещения.

Ключевые слова: маскирование информации; скрытая передача

Для цитирования: Закалкин П.В., Иванов С.А., Вершенник Е.В., Кирьянов А.В. Способ маскирования передаваемой информации. Труды ИСП РАН, том 32, вып. 6, 2020 г., стр. 111-126. DOI: 10.15514/ISPRAS–2020–32(6)–9

Method of Masking Transmitted Information

[1] *P.V. Zakalkin, ORCID: 0000-0003-2946-2586 <pzakalkin@mail.ru>*
[1] *S.A. Ivanov, ORCID: 0000-0002-0528-276X <sa-ivanov@inbox.ru>*
[1] *E.V. Vershennik , ORCID: 0000-0003-3647-741X <sukhorukova_lena@mail.ru>*
[2] *A.V. Kir'yanov, ORCID: 0000-0001-6104-7433 <sa-ivanov@inbox.ru>*

[1] *Military Telecommunications Academy,*
3, Tikhoretsky pr., Saint-Peterburg, 194064, Russia
[2] *Academy of the Federal Guard Service of the Russian Federation,*
35, Priborostroitelnaia st., Orel, 302015, Russia

Abstract. The processes of globalization, the emergence and active development of cyberspace have led to the need to protect information transmitted in the framework of information exchange. Existing approaches to information protection, in particular its encryption, steganography, etc. from the point of view of information exchange have a number of unmasking features that, despite the undoubted reliability of these approaches, significantly reduce the secrecy of information transmission. The proposed article considers an approach that allows for the hidden transmission of protected information over open communication channels, by masking the transmitted information. The development of the proposed approach was carried out in stages. at the first stage, a method for masking the transmitted information was developed and patented. At the next stage, on the basis of the developed method, a functional model of client and server applications of the hidden information transmission complex is created. The transfer of masked information is proposed to be carried out using the developed protocol of hidden information transfer. The block diagram of the package of the proposed Protocol for transmitting hidden information, the implementation and use of the Protocol at the application level are presented in this paper. At the final stage, a software implementation of the proposed approach was developed and modeling of information exchange at different offset Windows was performed. the paper presents a functional model of the developed complex, a scheme of interaction of functional modules, and a block diagram of the proposed approach to masking the transmitted information. Increasing the secrecy of information transmission is provided by the procedure for converting a carrier message into a marker message by forming an offset window, as well as using an array of digital records to select the carrier message. The proposed approach allows you to use a smaller carrier message when increasing the window size and using a sliding window depending on the size of the information message, you can choose the optimal size of the carrier message and the offset window.

Keywords: concealment of information; hidden transfer

For citation: Zakalkin P.V., Ivanov S.A., Vershennik E.V., Kir'yanov A.V. Method of masking transmitted information. Trudy ISP RAN/Proc. ISP RAS, vol. 32, issue 6, 2020, pp. 111-126 (in Russian). DOI: 10.15514/ISPRAS-2020-32(6)-9

1. Введение

Интеграция сетей связи различных операторов с Единой сетью электросвязи Российской Федерации (ЕСЭ РФ), наряду со значительными удобствами и удешевлением процесса организации связи (нет затрат на строительство и обслуживание линий связи), способствовало тому, что нарушители активно применяют различные средства информационно-технических воздействий.

Защищать передаваемую (или хранимую) информацию от несанкционированного использования приходится во многих случаях. Это требуется при решении государственных, дипломатических, военных задач, в работе бизнеса (коммерции), при исследовании новых научно-технических проблем, при разработке оригинальных технологических процессов и устройств. Защищать информацию требуется при документообороте в государственных организациях и при ведении частной переписки. Современные телекоммуникационные технологии невозможно представить без защиты передаваемой информации [1-2].

Основным подходом к защите передаваемой информации является ее шифрование. Данный подход считается наиболее приемлемым и позволяет скрыть передаваемую информацию.

Более того, порядка 70-80 % (из которого 90 % трафик https) мирового трафика передается в зашифрованном виде и потенциальному нарушителю, для осуществления какого-либо воздействия, среди этого трафика необходимо найти нужный.

На первый взгляд подход с шифрованием информации не лишен недостатков, однако:

- крупные корпоративные структуры, банковская сфера, элементы критической инфраструктуры используют специализированные программно-аппаратные средства шифрования трафика (например, криптомаршрутизаторы);
- взлом и дальнейший анализ трафика HTTPS для высококвалифицированного нарушителя не составляет особого труда;
- нарушитель будет анализировать трафик, исходящий от специализированных программно-аппаратных средств.

Для высококвалифицированного нарушителя, проводящего целевые атаки, сам факт наличия аппаратуры, предусматривающей шифрование, является мощным демаскирующим признаком. При этом, тип применяемого средства шифрования и используемый им алгоритм определить не сложно – достаточно проанализировать служебный трафик при установлении соединения.

Потенциальный нарушитель будет стремится получить доступ к защищаемой информации или вывести из строя закрытые каналы связи (для предотвращения информационного обмена). Таким образом, само наличие закрытого канала связи является своеобразным сигналом того, что в нем с большой долей вероятности передается защищаемая информация. При всем этом, для обеспечения информационного взаимодействия крупных территориально разнесенных корпоративных структур, банковской сферы и т.д. используется множество закрытых каналов передачи информации, по которым могут передаваться сведения, содержащие как государственную и коммерческую тайну, так и конфиденциальную информацию [3-4].

Логичным выходом из сложившейся ситуации является скрытая передача защищаемой информации по открытым каналам связи. При этом наличие нарушителя накладывает некоторые ограничения в виде необходимости передачи трафика в открытом виде и по одному каналу связи, который потенциально может контролироваться нарушителем. В связи с этим возникает необходимость разработки и исследования новых систем со скрытой передачей информации.

2. Способы скрытой передачи информации

Для решения поставленной задачи в первую очередь была рассмотрена стеганография. Данный подход позволяет разместить в цифровых файлах-контейнерах достаточно большой объем информации без явного искажения изображения, наличием априорных сведений о размерах контейнера, существованием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации, проработанностью способов цифровой обработки изображений и цифровых форматов представления изображений [5-8]. Однако существенным недостатком является невозможность обеспечения скрытного информационного обмена в силу внесения изменений (преобразований) в цифровой файл-контейнер, которые могут быть детектированы с помощью известных программных продуктов стеганоанализа.

После этого были рассмотрены альтернативные подходы к скрытному обмену информацией [9-12]. Однако они либо использовали подходы основанных на стеганографии, либо требовали дополнительного оборудования и обладали не высокой скрытностью.

Наиболее подходящим к сложившимся условиям и наложенным ограничениям является «Способ скрытой передачи информации» Патент РФ № 2552145, однако и он обладает рядом недостатков. Основными из которых можно выделить: необходимость использования

нескольких каналов связи; в качестве несущего изображения возможно использовать только одно изображение; низкая информационная емкость маркерного сообщения; отсутствие возможности изменения окна смещения. Данные недостатки существенно снижают скрытность передачи информации за счет достаточно простых действий при скрытии информационного сообщения, но являются устранимыми.

3. Разработка функциональной модели программного комплекса маскирования передаваемой информации

В рамках решения этой проблемы была разработана функциональная модель и запатентован способ маскирования передаваемой информации [13], на основе которого был разработан программный комплекс [14]. На рис. 1, 2 представлена функциональная модель программного комплекса, отображающая особенности его функционирования и внутреннюю взаимосвязь элементов.

Прежде чем приступить к дальнейшему рассмотрению предлагаемого способа необходимо дать определения используемых терминов.

1) Информационное сообщение – сообщение, предназначенное для передачи абоненту и являющееся цифровой записью в двоичном виде.
2) Несущее сообщение – сообщение, которое представляет собой цифровую запись в двоичном виде, являющуюся реальными файлами соответствующих расширений. Например, для аудио файлов расширения: .mp3, .ac3, .3ga и т.д., для видеофайлов .mp4, .mpg, .mkv и т.д.
3) Маркерное сообщение – цифровая запись в двоичном виде, полученная после маскирования информационного сообщения с помощью несущего сообщения и предназначенная для передачи по каналу связи.
4) Маркерный пакет – пакет, передаваемый по каналу связи и включающий в себя заголовок и маркерное сообщение.

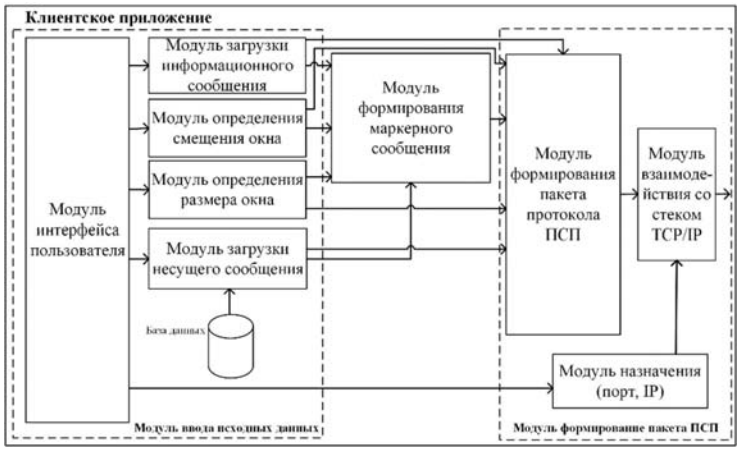

Рис. 1. Функциональная модель клиентского приложения разработанного программного комплекса передачи скрытой информации

Fig. 1. Functional model of a client application developed by a software package for transmitting hidden information

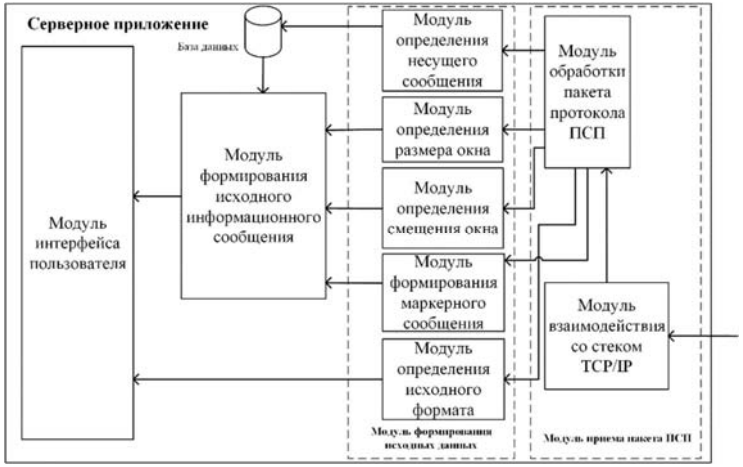

Рис. 2. Функциональная модель серверного приложения разработанного программного комплекса передачи скрытой информации

Fig. 2. Functional model of a server application developed by a software package for transmitting hidden information

Разработка функциональной модели является одним из основных этапов проектирования систем и предназначена для изучения особенностей работы системы до её программной, аппаратной или программно-аппаратной реализации. Функциональная модель является абстрактной моделью создаваемой системы и содержит все необходимые элементы разрабатываемой системы, а также их взаимосвязь и взаимодействие как между собой, так и с окружающими объектами.

Разработанная функциональная модель включает 2 основных модуля:

- серверное приложение;
- клиентское приложение.

«Модуль взаимодействия со стеком TCP/IP» предназначен для приема всего трафика от клиентского приложения, выделения метки времени, а также выделения информации об адресе отправителя и номере порта для каждого пакета и дальнейшей передачи пакета на соответствующий модуль.

«Модуль обработки пакета протокола скрытой передачи информации (ПСП)» принимает информацию от модуля взаимодействия со стеком TCP/IP, а также осуществляет распределение информации на модули формирования маркерного сообщения, определения размера окна, определения смещение окна, определения несущего сообщения, определения исходного формата.

«Модуль формирование маркерного сообщения» принимает последовательность бит с модуля обработки пакета ПСП, выстраивает их в правильной последовательности и осуществляет ее передачу на модуль формирования исходного информационного сообщения.

«Модуль определения размера окна» принимает данные с модуля обработки пакета ПСП. В данном модуле собирается характеристика о размере окна, которая была задана в клиентском приложении для формирования маркерного сообщения.

«Модуль определения смещения окна» принимает данные с модуля обработки пакета ПСП. В данном модуле собирается характеристика о смещении окна, которая была задана в клиентском приложении для формирования маркерного сообщения.

«Модуль определения исходного формата» принимает информацию с модуля обработки пакета ПСП. В данном модуле определяется информация о формате переданного сообщения с клиентского приложения, например, doc, jpeg и т.п.

«Модуль определения несущего сообщения» принимает информацию с модуля обработки пакета ПСП. В данном модуле определяется информация о номере несущего сообщения, хранящегося в базе данных. Информация о несущем сообщении нужна для того, чтобы получить правильное информационное сообщение.

«Модуль формирования исходного информационного сообщения» принимает данные от модулей формирования маркерного сообщения, определения смещения окна, определения размера окна, определения несущего сообщения и с базы данных. В результате применения алгоритма извлечения информационного сообщения из маркерного мы получаем исходное сообщение, которое передавалось с клиентского приложения.

«Модуль формирования информационного сообщения» принимает данные с модуля формирования исходного информационного сообщения. В результате мы получаем файл, который передавался с клиентского приложения.

«Модуль интерфейса пользователя» предназначен для осуществления взаимодействия с пользователем и установки исходных данных, а также для последующего формирования кадров, необходимых для настройки модуля взаимодействия клиент/сервера.

«База данных» содержит множество различных файлов, с помощью которых в алгоритме сокрытия конфиденциальной информации формируется несущее сообщение.

«Модуль назначения» отвечает за передачу на модуль взаимодействия со стеком TCP/IP таких характеристик, как номер порта назначения и IP адрес.

Схема взаимодействия функциональных модулей представлена на рис. 3.

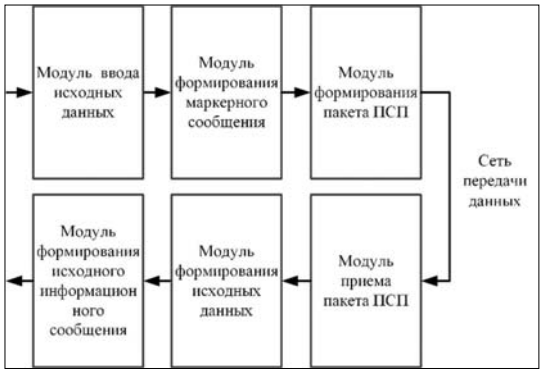

Рис. 3. Схема взаимодействия функциональных модулей

Fig. 3. Scheme of interaction of functional modules

Клиентское приложение в свою очередь состоит из следующих модулей:

- модуль взаимодействия со стеком TCP/IP;
- модуль обработки пакета ПСС;
- модуль интерфейса пользователя;
- модуль загрузки информационного сообщения;
- модуль определения размера окна;
- модуль загрузки несущего сообщения;
- модуль формирование маркерного сообщения;
- модуль определения смещения окна;
- модуль назначения;

- база данных.

Несмотря на некоторую тривиальность отдельных блоков, для удобства восприятия блок-схема предлагаемого способа маскирования информации (рис. 4.) представлена в более подробном виде.

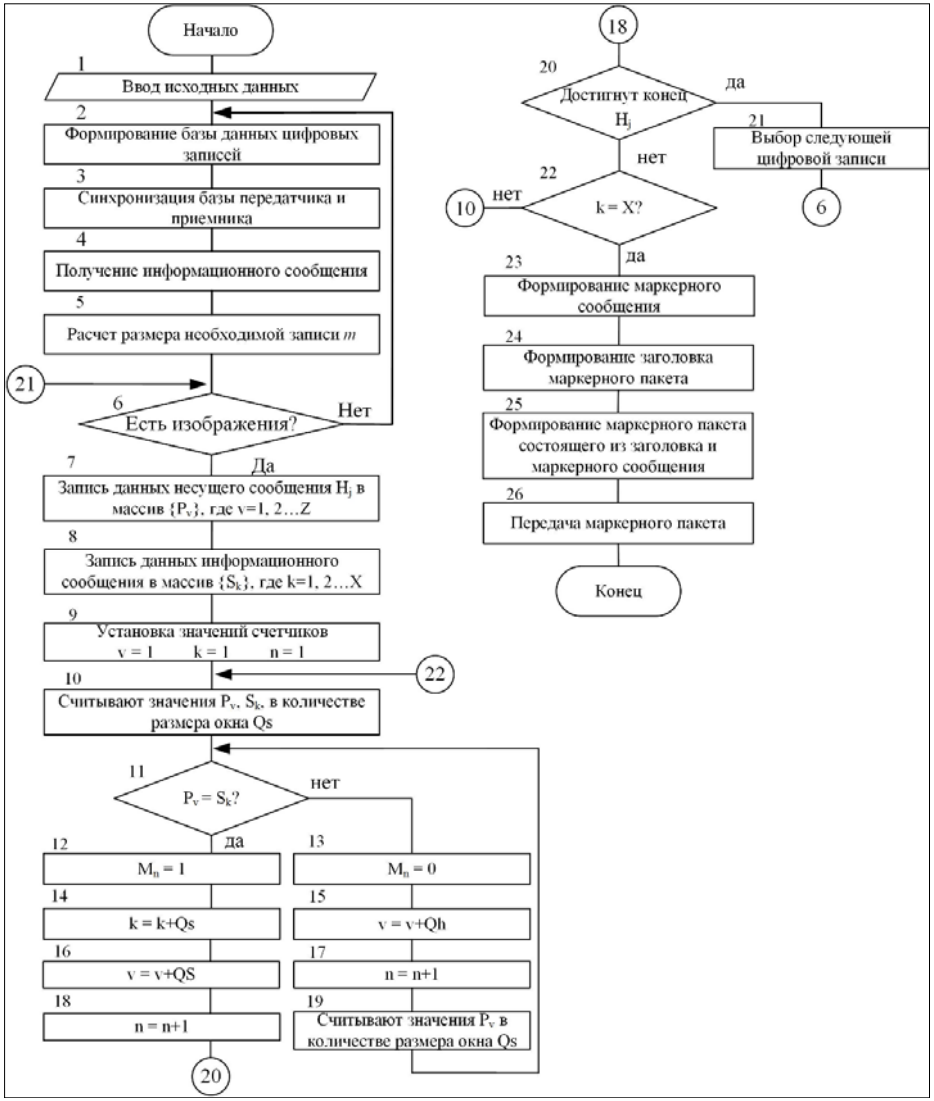

Рис. 4. Блок-схема способа маскирования передаваемой информации
Fig. 4. Block diagram of the method for masking transmitted information

На первоначальном этапе маскирования передаваемой информации осуществляют задание исходных данных:

Qh – значение маркера смещения несущего сообщения;

Qs – размер окна смещения информационного сообщения.

Кроме того, формируют массивы для запоминания битовой последовательности информационного сообщения $\{S_k\}$, где $k = 1, 2, \dots, X$, битовой последовательности несущего сообщения $\{P_v\}$, где $v = 1,2, \dots, Z$, битовой последовательности маркерного сообщения $\{M_n\}$, где $n = 1, 2, \dots, Y$.

После этого осуществляют формирование базы данных цифровых записей в виде видео-, аудио-файлов (информация) и т.д. База данных цифровых записей (несущих сообщений) $\{B\}$ состоит из массива несущих сообщений $\{H_j\}$; в свою очередь, несущее сообщение состоит из последовательности бит $\{h_v\}$.

Далее синхронизируют базу передающего и принимающего абонента. В процессе синхронизации сравниваются все цифровые записи в базах данных передающего и принимающего абонентов. При необходимости осуществляется дополнение цифровых записей в базах для достижения полной идентичности баз данных. Базы считаются синхронизированными, если все цифровые записи в базах данных отправителя и получателя совпадают.

Создание базы данных и входящих в нее цифровых записей осуществляется по предварительной договоренности корреспондентов любым удобным для них способом. Например, возможен обмен базами данных на flash, CD и т.д. носителях. Возможно скачивание цифровых записей из социальных сетей, со сторонних ресурсов, например, FTP сервера содержащие исходные тексты программного обеспечения, содержат множество файлов различных форматов (при этом все они имеют контрольные суммы) и т.д. Таким образом, даже при полном контроле трафика потенциальным злоумышленником процесс формирования и синхронизации базы данных будет выглядеть как обычная активность пользователей в офисе (просмотр соцсетей, e-mail, загрузка аудио и видео файлов и т.д.).

Информационное сообщение, которое необходимо передать, представляется в цифровом виде, позволяющем в блоке 9 (рис. 4) записать его в массив $\{S_k\}$, где $k = 1, 2, \dots, X$.

Для осуществления передачи информационного сообщения рассчитывают размер необходимой цифровой записи, которая далее будет использоваться как несущее сообщение H_j. Учитывая размеры информационного и несущего сообщений (при большом количестве испытаний), в соответствии с предельной теоремой, суммарный закон распределения случайных величин будет соответствовать нормальному закону. Таким образом, для определения объема несущего сообщения, необходимого для переноса информационного сообщения используется выражение:

$$P_v \geq S_n \cdot 2^{Qs},$$

где P_v – массив, содержащий битовую последовательность несущего сообщения; S_n – массив, содержащий битовую последовательность информационного сообщения; Qs – размер окна смещения для информационного сообщения.

Из базы данных выбирают цифровую запись, превышающую по размеру рассчитанное значение несущего сообщения, но при этом наиболее близкую по размеру. Выбранная таким образом цифровая запись будет иметь превышение размера для обеспечения преобразования текущего информационного сообщения. В случае, если цифровая запись необходимого размера в базе данных не обнаружена, то формируют дополнительные цифровые записи и записывают их в базу данных цифровых записей с учетом рассчитанного размера несущего сообщения.

Битовые последовательности несущего сообщения H_j записывают в массив $\{P_v\}$, где $v = 1,2, \dots, Z$, а битовые последовательности информационного сообщения записывают в массив $\{S_k\}$, где $k = 1, 2, \dots, X$.

После этого последовательно считывают из соответствующих массивов значения P_v и S_k в количестве, равном размеру окна смещения Qs и осуществляют сравнение считанных

битовых последовательностей несущего и информационного сообщений P_v и S_k. При совпадении данных битовых последовательностей флаговое значение M_n устанавливают в «единицу», в противном случае флаговое значение M_n устанавливают в «ноль» (рис. 5).

Рис.5. Схема, поясняющая процесс формирования маркерного сообщения
Fig.5. Diagram explaining the process of forming a marker message

Значение счетчика k увеличивают на размер окна смещения для информационного сообщения Qs:

$$k = k + Qs.$$

Это соответствует переходу и анализу следующих по порядку битовых последовательностей информационного сообщения, сдвинутых на размер окна смещения информационного сообщения.

Значение счетчика v увеличивают на значение маркера смещения для несущего сообщения Qh:

$$v = v + Qh.$$

Это соответствует переходу и анализу следующих по порядку битовых последовательностей информационного сообщения, сдвинутых на значение маркера смещения несущего сообщения.

Значение счетчика v увеличивают на размер окна смещения для информационного сообщения Qs:

$$v = v + Qs.$$

Значение счетчика n увеличивают на «единицу» $n = n + 1$ для формирования следующих битовых значений маркерного сообщения.

После чего считывают значения следующей битовой последовательности P_v в количестве размера окна Qs и переходят к блоку 12 (рис. 4), где сравнивают битовые последовательности несущего и информационного сообщений P_v и S_k.

В случае достижения окончания несущего сообщения из базы данных цифровых записей в качестве несущего сообщения выбирают цифровую запись, превышающую по размеру текущую, но при этом наиболее близкую к ней по размеру.

При достижении окончания информационного сообщения формируют маркерное сообщение, представляющее собой битовую последовательность Mn, состоящее из записанных флаговых значений «ноль» и «единица», которое было сформировано в блоках 12 и 13 (рис. 4).

Для передачи маркерного пакета по каналу связи формируют заголовок маркерного пакета, состоящий из номеров выбранных цифровых записей, размера окна смещения Qs и значения маркера смещения Qh. После чего формируют маркерный пакет, состоящий из заголовка и маркерного сообщения, и записывают его в информационное поле пакета передаваемого по сети связи.

Передачу маркерного сообщения предлагается осуществлять с помощью протокола скрытой передачи информации, структурная схема пакета которого представлена на рис. 6.

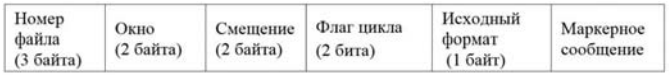

Рис. 6. Структурная схема пакета протокола передачи скрытой информации
Fig. 6. Block diagram of the hidden information transfer Protocol package

Структурная схема пакета протокола скрытой передачи информации предусматривает следующие поля для данного протокола: номер файла; размер окна; размер смещения; флаг цикла; исходный формат; маркерное сообщение.

- Номер файла – поле, предназначенное для передачи информации о примененном файле несущего сообщения. Размер поля 3 байта.
- Размер окна – поле, показывающее, какое количество бит сравнивается в алгоритме сокрытия информации. Размер поля 2 байта.
- Смещение – поле, в котором указывается количество бит смещения при формировании маркерного сообщения. Размер поля 2 байта.
- Флаг цикла – поле, которое показывает, что применялось циклическое использование одного несущего сообщения. Размер поля 2 бита.
- Исходный формат – поле, которое указывает, в каком исходном формате было информационное сообщение (doc, jpeg, и т.п.). Размер поля 1 байт. Обозначение форматов для заполнения поля представлено в табл. 1.

Табл. 1. Обозначение форматов в поле исходный формат
Table. 1. The designation of the formats in the original format

Формат	**Обозначение**	**Формат**	**Обозначение**
.jpg	00000000	.png	00001001
.docx	00000001	.ico	00001010
.mp4	00000010	.bmp	00001011
.gif	00000011	.xmcd	00001100
.pdf	00000100	.log	00001101
.vsd	00000101	.db	00001110
.txt	00000110	.md	00001111
.doc	00000111	.fb2	00010000
.pptx	00001000		

Наличие нестандартного протокола передачи (протокол скрытой передачи информации) будет серьезным демаскирующим признаком для системы связи любой организации его использующей. Однако, принимая во внимание принцип инкапсуляции протоколов,

предлагается использовать протокол не на сетевом или транспортном уровне, а на прикладном (рис. 7). Это позволит использовать любой протокол прикладного уровня для переноса в поле данных вложенного протокола передачи скрытой информации.

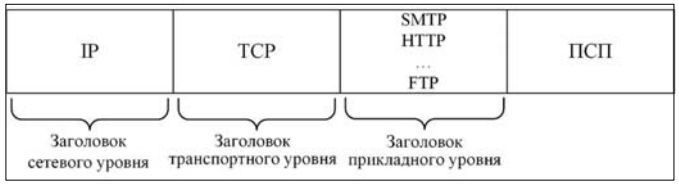

Рис. 7. Графическое отображение инкапсуляции пакета протокола скрытой передачи информации на примере стека протоколов TCP/IP
Fig. 7. Graphical representation of the encapsulation of a packet of the hidden information transfer protocol on the example of the TCP / IP Protocol stack

При анализе сетевого трафика злоумышленник будет видеть TCP/IP пакеты в незашифрованном виде, при этом параметры трафика будут абсолютно не отличимыми от стандартного трафика при любом другом информационном обмене. Учитывая большие объемы открытого трафика и отсутствие какой-либо априорной информации о том, с кем идет информационный обмен и что необходимо искать в передаваемом трафике (протоколы прикладного уровня), задача найти TCP/IP пакеты, содержащие в себе пакеты протокола скрытой передачи информации сравнима с задачей поиска иголки в стоге сена.

Для моделирования размеров передаваемых файлов, типовых сообщений, Web-страниц часто используется распределение Парето, которое имеет следующий вид

$$w(x) = \frac{\alpha k^{\alpha}}{x^{\alpha+1}}, \alpha > 0, k > 0, x > 0, \quad (1)$$

Где α – параметр формы; k – параметр, определяющий нижнюю границу для случайной величины.

С помощью ЭВМ возможно генерировать равномерно распределенную случайную величину y в диапазоне от 0 до 1. Для того чтобы моделировать случайную величину x с плотностью распределения вероятности Парето, необходимо найти функциональное преобразование $x = f(y)$.

Это можно сделать на основе выражения

$$w(x = f(y)) = w(y)\left|\frac{dy}{dx}\right|, \quad (2)$$

откуда

$$y = \int w(x)dx = \int \frac{\alpha k^{\alpha}}{x^{\alpha+1}}dx = 1 - \left(\frac{k}{x}\right)^{\alpha}, \quad (3)$$

при $x > k$, $\alpha > 0$.

Таким образом, получаем следующее выражение для моделирования случайной величины с плотностью распределения вероятности Парето:

$$x = \frac{k}{\sqrt[\alpha]{1 - rand}}, \quad (4)$$

где $rand$ – случайное число, подчиненное равномерному закону распределения, генерируемое на ЭВМ в диапазоне от 0 до 1. Параметр α связан с показателем Херста выражением $\alpha = 3 - 2H$.

Параметр α обычно вычисляется на основе метода максимального правдоподобия по известным результатам измерения интенсивности реального трафика $X = [x_1, x_2, \dots, x_n]$:

$$\alpha = \frac{n-1}{\sum_{i=1}^{n} logX_i - nlogk}, \quad (5)$$

где $k = \min_i k$.

На практике значение параметра самоподобия находится в промежутке от 1\2 до 3\2. Таким образом, можно осуществить моделирование размеров как несущих сообщений, так и информационных сообщений. Более важную роль будет играть отношение размера несущего сообщения к информационному сообщению ($L_{НС}/L_{ИС}$).

Из логики функционирования способа следует, что при малом несущем сообщении и большом информационном сообщении, алгоритм не будет сходиться. Поэтому необходимо определить $G_{ДОП} > (L_{НС}/L_{ИС})$ – границу, при которой размера несущего сообщения будет достаточно для нахождения отображения в нем информационного сообщения, либо рассмотреть вариант формирования последовательности нескольких несущих сообщений для переноса информации одного сообщения.

Так как появление в сообщениях битов «0» и «1» подчиняется равномерному закону, то можно сделать предположение о том, что композиция двух законов равномерной плотности распределения, заданных на одном и том же участке, будет соответствовать закону распределения Симпсона (иначе «закон треугольника») [15].

Однако, учитывая размеры сообщений $L_{ИС}$ и $L_{НС}$ (при большом количестве испытаний), в соответствии с предельной теоремой, суммарный закон распределения случайных величин будет соответствовать нормальному закону.

В ходе исследования и практической реализации способа получены результаты, подтверждающие гипотезу. Количество испытаний для каждого размера окна $N_{исп} = 20000$. На рис. 8 показана зависимость частоты совпадений отношения объема информационного сообщения к объему маркерного сообщения.

Таким образом, для определения объема несущего сообщения $L_{НС}$, необходимого для переноса информационного сообщения $L_{ИС}$, было получено выражение

$$L_{НС} \geq L_{ИС} \cdot 2^{L_{окна}}.$$

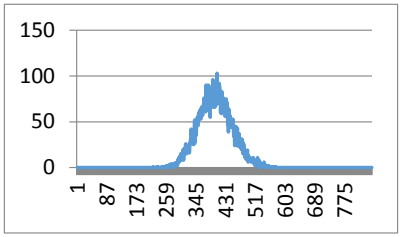

Рис. 8. Зависимость частоты совпадений отношения объема информационного сообщения к объему маркерного сообщения (Локна = 2, Vинф = 200)
Fig. 8. Dependence of the frequency of matches of the ratio of the volume of the information message to the volume of the marker message (Локна = 2, Vинф = 2000)

В табл. 2 представлены статистические данные соответствия размера информационного сообщения размеру несущего сообщения при величине окна сравнения 2 и 3 бита.

Табл. 2. Результаты моделирования при смещении окна на $L_{окна}$
Table. 2.– Simulation results when the window is shifted by $L_{окна}$

$L_{ИС}$	$L_{окна}$	$L_{МС}$	$L_{НС}$	$L_{окна}$	$L_{МС}$	$L_{НС}$
100	2	200	400	3	267	800
200	2	400	800	3	533	1600
300	2	600	1200	3	800	2400
400	2	800	1600	3	1067	3200
500	2	1000	2000	3	1333	4000

Дальнейшее исследование проводилось в направлении реализации процедуры скользящего окна. При реализации алгоритма со скользящим окном, смещение окна производится не на размер окна, а на один бит. При этом размер маркерного сообщения увеличивается – каждому биту несущего сообщения ставится в соответствие бит маркерного сообщения. Информационная емкость несущего сообщения увеличивается. Результаты моделирования представлены в табл. 3.

Табл. 3. Результаты моделирования при смещении окна на 1 бит (скользящее окно)

Table. 3. Simulation results when the window is shifted by 1 bit (sliding window)

$L_{ИС}$	$L_{окна}$	$L_{МС}$	$L_{НС}$	$L_{окна}$	$L_{МС}$	$L_{НС}$	$L_{окна}$	$L_{МС}$	$L_{НС}$
100	2	179	179	3	278	278	4	391	391
200	2	387	387	3	530	530	4	785	785
300	2	591	591	3	786	786	4	1189	1189
400	2	795	795	3	1078	1078	4	1570	1570
500	2	989	989	3	1317	1317	4	1934	1934

Таким образом, предлагаемый способ позволяет при увеличении размера окна и использовании скользящего окна использовать меньшее несущее сообщение. Помимо этого, в зависимости от размера информационного сообщения выбирать оптимальный размер несущего сообщения и окна смещения.

Необходимо понимать, что увеличивать размер окна до бесконечности нельзя и при многократном увеличении размера окна, произойдет кардинально противоположная ситуация и размер несущего сообщения будет несоизмеримо больше размера информационного сообщения.

Основными этапами функционирования разработанного программного комплекса [14] являются следующие:

1) выполняется считывание входных параметров, на основе которых строится вся дальнейшая работа алгоритма;
2) исходное сообщение преобразовывается в маркерное сообщение;
3) устанавливается соединение клиента и сервера, осуществляется синхронизация баз данных;
4) сообщения делятся на пакеты и передаются в зашифрованном виде по каналу связи;
5) принимается последний пакет и осуществляется разъединение между клиентом и сервером;
6) из принятых пакетов извлекаются основные параметры алгоритма маскирования передаваемой информации;
7) маркерное сообщение преобразуется в исходное сообщение;
8) полученное сообщение сохраняется в удобном формате, исходя из требований пользователя.

Основными функциональными возможностями программного комплекса являются:

- передача сообщения в скрытом виде;
- выбор режима (автоматически, самостоятельно) изменения основных параметров алгоритма сокрытия информации, таких как размер окна и смещение окна;
- возможность добавления различных узлов;
- передача текста, цифровых записей различного формата.

4. Заключение

Представленные в работе исследования, посвященные разработке способа маскирования передаваемой информации [13], программного комплекса [14] и протокола скрытой передачи

информации позволяют осуществлять передачу защищаемой информации по открытым каналам связи, а также, в зависимости от размера передаваемого информационного сообщения, можно выбирать оптимальный размер окна и его смещение.

Список литературы / References

[1]. Цыцулин А.К., Зубакин И.А. Концепция качества информации в теории связи. Вопросы радиоэлектронники. Серия: Техника телевидения, № 4, 2016 г. стр. 19-25 / Tsyculin A.K., Zubakin I.A. Quality information concept in the theory of communication. Voprosy radiojelektronniki. Serija: tehnika televidenija, № 4, 2016, pp. 19-25 (in Russian).

[2]. Коцыняк М.А., Кулешов И.А., Кудрявцев А.М., Лаута О.С. Киберустойчивость информационно-телекоммуникационной сети. СПб., Бостон-спектр, 2015 г., 150 стр. / Kotsynjak M.A., Kuleshov I.A., Kudrjavtsev A.M., Lauta O.S. Cyber stability of the information and telecommunications network. SPb., Boston-spektr, 2015, 150 p. (in Russian).

[3]. Бегаев А.Н., Гречишников Е.В., Добрышин М.М., Закалкин П.В. Предложение по оценке способности узла компьютерной сети функционировать в условиях информационно-технических воздействий. Вопросы кибербезопасности, № 3(27), 2018 г., стр. 2-8. / Begaev A.N., Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. Proposal for assessing the ability of a computer network node to function in conditions of information and technical influences. Voprosy kiberbezopasnosti, № 3 (27), 2018, pp. 2-8(in Russian).

[4]. Гречишников Е.В., Добрышин М.М., Закалкин П.В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDOS-атак. Вопросы кибербезопасности, № 3(16), 2016 г., стр. 4-12 / Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. A model of a VPN access point as of an object of network and streaming computer intelligence and DDOS attacks. Voprosy kiberbezopasnosti, № 3(16), 2016, pp.4-12(in Russian).

[5]. Цветков К.Ю., Федосеев В.Е., Коровин В.М., Абазина Е.С. Способ скрытой передачи данных в видеоизображении. Патент на изобретение RUS 2608150, опубл. 16.01.2017, 19 стр. / Cvetkov K.Ju., Fedoseev V.E., Korovin V.M., Abazina E.S. Method for hidden data transfer in a video image. Patent for invention RUS 2608150, published 16.01.2017, 19 p. (in Russian).

[6]. Галушка В.В., Петренкова С.Б., Дзюба Я.В., Панченко В.А. Сетевая стеганография на основе ICMP-инкапсуляции. Инженерный вестник Дона, №4(51), 2018 г., стр. 107-118. / Galushka V.V., Petrenkova S.B., Dzjuba Ja.V., Panchenko V.A. Network steganography based on ICMP-encapsulation. Engineering journal of Don, №4(51), 2018, pp.107-118 (in Russian).

[7]. Стародубцев Ю.И., Закалкин П.В., Мартынюк И.А. Способ скрытного информационного обмена. Вопросы радиоэлектронники. Серия: Техника телевидения, №1, 2020 г., стр. 57-63. / Starodubcev Ju.I., Zakalkin P.V., Martynjuk I.A. Method of secret information exchange. Voprosy radiojelektronniki. Serija: tehnika televidenija, №1, 2020, pp. 57-63 (in Russian).

[8]. Иванов В.А., Снаров М.М., Двилянский А.А., Иванов И.В., Кирюхин Д.А., Крюков М.С., Ксенофонтов А.А., Щуров К.С. Способ встраивания информации в графический файл, сжатый фрактальным методом. Патент на изобретение RUS 2602670, опубл. 20.11.2016, 11 стр. / Ivanov V.A., Snarov M.M., Dviljanskij A.A., Ivanov I.V., Kirjuhin D.A., Krjukov M.S., Ksenofontov A.A., Shhurov K.S. A method of embedding information into a graphic file is compressed fractal method. Patent for invention RUS 2602670, published 20.11.2016, 11 p. (in Russian).

[9]. Короновский А.А., Москаленко О.И., Храмов А.Е. Способ скрытой передачи информации. Патент на изобретение RUS 2349044, опубл. 10.03.2009, 8 стр. / Koronovskij A.A., Moskalenko O.I., Khramov A.E. Secure information transmission method, Patent for invention RUS 2349044, published 10.03.2009, 8 p. (in Russian).

[10]. Москаленко О.И., Фролов Н.С., Короновский А.А., Храмов А.Е. Способ скрытой передачи информации. Патент на изобретение RUS 2509423, опубл. 10.03.2014, 11 стр. / Moskalenko O.I., Frolov N.S., Koronovskij A.A., Khramov A.E. Secure information transmission method. Patent for invention RUS 2349044, published 10.03.2009, 11 p. (in Russian).

[11]. Алексеев А.П., Макаров М.И. Способ скрытой передачи зашифрованной информации по множеству каналов связи. Патент на изобретение RUS 2462825, опубл. 27.09.2012, 39 стр. / Moskalenko O.I., Frolov N.S., Koronovskij A.A., Khramov A.E. Method of hidden transfer of coded information along multiple communication channel. Patent for invention RUS 2462825, published 27.09.2012, 39 p.

[12]. Котцов В.А., Котцов П.В. Способ скрытой передачи цифровой информации. Патент на изобретение RUS 2636690, опубл. 09.12.2016, 13 стр. / Kottsov V.A., Kottsov P.V. Method of hidden transferring digital information. Patent for invention RUS 2636690, published 09.12.2016, 13 p.

[13]. Бухарин В.В., Закалкин П.В., Кирьянов А.В., Стародубцев Ю.И. Способ маскирования передаваемой информации. Патент на изобретение RUS 2660641, опубл. 06.07.2018, 13 стр. / Buharin V.V., Zakalkin P.V., Kir'janov A.V., Starodubcev Yu.I. Method of masking transmitted information. Patent for invention RUS 2660641, published 06.07.2018, 13 p.

[14]. Закалкин П.В., Кирьянов А.В., Приходько А.В., Манзюк В.В. Программа маскирования передаваемой информации. Свидетельство о государственной регистрации программ для ЭВМ RU 2019618344. / Zakalkin P.V., Kir'janov A.V., Prihod'ko A.V., Manzjuk V.V. Program for masking transmitted information. Certificate of state registration of computer programs RU 2019618344.

[15]. Вентцель Е.С. Теория вероятностей. М., Академия, 2003 г., 576 стр. / Wentzel' E.S. Probability theory. M., Academy, 2003, 576 p. (in Russian).

Информация об авторах / Information about authors

Павел Владимирович ЗАКАЛКИН – кандидат технических наук, докторант. Научные интересы: информационная безопасность, безопасность компьютерных сетей.

Pavel Vladimirovich ZAKALKIN – Candidate of Technical Sciences, doctoral candidate. Research interests: information security, computer network security.

Сергей Александрович ИВАНОВ – кандидат технических наук, докторант. Сфера научных интересов: теория управления информационно-телекоммуникационными ресурсами, инфотелекоммуникационные системы и их подсистемы обеспечения.

Sergei Aleksandrovich IVANOV – Candidate of Technical Sciences, doctoral candidate. Research interests: theory of information and telecommunication resources management, infotelecommunication systems and their support subsystems.

Елена Валерьевна ВЕРШЕННИК – кандидат технических наук, преподаватель. Научные интересы: информационная безопасность, криптографические методы защиты информации.

Elena Valer’evna VERSHENNIK – Candidate of Technical Sciences, lecturer. Research interests: information security, cryptographic methods of information protection.

Александр Владимирович КИРЬЯНОВ – кандидат технических наук. Сфера научных интересов: безопасность компьютерных сетей, инфотелекоммуникационные системы и их подсистемы обеспечения.

Aleksandr Vladimirovich KIR’YANOV – Candidate of Technical Sciences. Research interests: security of computer networks, info-telecommunications systems and their supporting systems.