ОБЗОР СОВРЕМЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЮЩЕГО МЕТОДЫ СТЕГАНОГРАФИИ

Е.Ю. Герлинг, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerlingeu@gmail.com;*
К.А. Ахрамеева, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksenya_2002@mail.ru.*

УДК 004.056.5

Аннотация. В статье представлен результат исследования программного обеспечения, использующего методы стеганографии. Описаны примитивные методы вложения информации. Рассмотрено стеганографическое программное обеспечение, широко распространенное в сети интернет. Освещены основные типы контейнеров и алгоритмы вложения, используемые в программах. Сделаны выводы о надежности такого программного обеспечения.

Ключевые слова: стеганография; программное обеспечение; контейнер; вложение информации.

THE REVIEW OF THE MODERN SOFTWARE USING STEGANOGRAPHY METHODS

Ekaterina Gerling, *candidate of technical science, associate professor, St. Petersburg state university of telecommunications n/a prof. M. A. Bonch-Bruevich;*
Kseniya Ahrameeva, *candidate of technical science, associate professor, St. Petersburg state university of telecommunications n/a prof. M. A. Bonch-Bruevich.*

Annotation. The article presents the result of a study of software using steganography methods. Primitive methods for embedding information are described. The steganographic software widely distributed on the Internet is considered. The main types of containers and attachments algorithms used in the programs are highlighted. Conclusions are made about the reliability of such software.

Keywords: steganography; software; container; information embedding.

Введение

Во все времена у человечества существовали тайны, которые нуждались в сокрытии, существовала информация, которую необходимо было передать союзникам таким образом, чтобы враг не смог ее прочитать. В скрытом от посторонних глаз обмене информации нуждались торговцы, военные, государственные деятели, заговорщики и многие другие. От надежности сокрытия сообщений зависели успехи в торговых делах, исход войны, а иногда и жизнь людей.

Для сокрытия секретной информации как раньше, так и сейчас, используется криптография. Методы криптографии позволяют зашифровать сообщение таким образом, чтобы посторонний не мог его прочитать. Однако, при передачи такого сообщения, сторонний наблюдатель будет точно знать, что происходит передача зашифрованного сообщения, что вызовет дополнительный интерес, который нежелателен для передающей и принимающей стороны. Если передаваемое сообщение выглядит подозрительно, то у стороннего наблюдателя (атакующего) возникнет желание расшифровать данное сообщение, и в некоторых случаях у него это получится. А значит, секретная информация будет перехвачена и потеряет свою ценность и актуальность.

Во избежание подобных ситуаций используются методы стеганографии, позволяющие скрыть сам факт передачи секретной информации. При использовании стеганографических методов сокрытия информации сторонний наблюдатель даже не заподозрит, что идет обмен информацией, поскольку секретное сообщение будет надежно спрятано от его взора в неприметном сообщении.

В современном мире активно развиваются компьютерные технологии и цифровые каналы коммуникаций, а информация часто представлена в виде медиафайлов. Поэтому помимо древних методов стеганографии появилась цифровая стеганография, использующая медиафайлы для передачи секретной информации. Медиафайлы используются как контейнеры, в которые помещается скрываемая информация. Невооруженным взглядом обнаружить секретную информацию невозможно, поэтому медиафайлы с вложенной в них скрытой информацией можно смело передавать по открытым каналам связи.

Методы цифровой стеганографии позволяют спрятать секретную информацию в обычные медиафайлы, которые потом могут хранится на компьютере или любом другом носителе информации, передаваться как по защищенным каналам связи, так и по общедоступным, таким как сеть интернет, и даже размещаться на интернет-ресурсах, где будут доступны широкой массе людей. Поскольку медиафайлы содержат секретную информацию, вложенную методами стеганографии, для стороннего наблюдателя файлы с вложениями будут выглядеть абсолютно невинно и не вызовут подозрений.

Отметим, что в современном мире методы стеганографии часто используются преступниками и террористами для обмена информацией и координации действий. Например, по мнению специалистов [1], террористы, связанные с Усама бен Ладеном и группировкой Аль-Кайда обменивались информацией с использованием программного обеспечения, использующего алгоритмы стеганографии.

Если у людей есть потребность скрывать информацию, то есть и потребность находить эту скрытую информацию. Поиск секретной информации в медиафайлах выполняется с помощью алгоритмов стегоанализа (стегоатаки), которые по статистическим данным медиафайла оценивают, есть ли в нем вложение или нет.

Поскольку, как отмечалось ранее, преступники и террористы все чаще используют методы стеганографии в незаконных целях, при этом используют открытые каналы для обмена информацией. Разработка методов выявления медиафайлов, содержащих скрытое вложение, среди большого потока невинных объектов на сегодняшний день является актуальной задачей.

При разработке методов стеганографии и стегоанализа принято считать, что атакующий знает:

- модель стегосистемы, то есть алгоритмы вложения и извлечения информации, если они не являются частью ключа;
- общие статистические свойства контейнера. Стоит отметить, что атакующий никогда не должен знать в точности контейнера, иначе становится возможным тривиальная атака по обнаружению скрытой информации путем сравнения контейнера и исследуемого (проверяемого) объекта.

На сегодняшний день существует множество методов вложения секретной информации в различные медиафайлы. Для более ясного понимания о методах погружения информации в контейнеры опишем базовые алгоритмы погружения.

Представим медиафайлы, используемые как контейнеры, в виде последовательности L-битовых отсчетов. Тогда цифровое значение n-го отсчета контейнера имеет вид [2]:

$$C(n) = \sum_{i=0}^{L-1} C_i(n) 2^i, \qquad (1)$$

где: $C_i(n) \in 0,1,\ i = 0,1,\ldots,L-1$ определяет значение i-го бита.

Вложение информации в наименьший значащий бит (НЗБ) [3] называется алгоритм, при котором наименьший значащий бит, содержащийся в отсчете контейнера $C(n)$, заменяется информационным битом скрываемого сообщения:

$$C_w(n) = \sum_{i=1}^{L-1} C_i(n) \cdot 2^i + b(n), \qquad (2)$$

где: $b(n)$ – бит, вложенный в n-й отсчет;

$C_w(n)$ – отсчеты контейнера с вложенной дополнительной информацией.

Еще одним из распространенных на сегодняшний день алгоритмов вложения – *F*5 [3], является модификация НЗБ. В данном методе, для того, чтобы вложить биты x_1, x_2, можно менять биты a_1, a_2, a_3. Тогда вложения производятся по следующим правилам:

$x_1 = a_1 \oplus a_3$, $x_2 = a_2 \oplus a_3$ => контейнер остается в исходном виде,
$x_1 \neq a_1 \oplus a_3$, $x_2 = a_2 \oplus a_3$ => необходимо изменять a_1, (3)
$x_1 = a_1 \oplus a_3$, $x_2 \neq a_2 \oplus a_3$ => необходимо изменять a_2,
$x_1 \neq a_1 \oplus a_3$, $x_2 \neq a_2 \oplus a_3$ => необходимо изменять a_3.

Рассмотренные выше методы недостаточно хорошо защищены от атаки удаления. Для защиты от этой атаки необходимо использовать, так называемые широкополосные сигналы (ШПС) [3]. В этом случае каждый бит информации передается при помощи последовательности, состоящей из N_0 элементов. Вложения ШПС производится по алгоритму:

$$C_w(n) = C(n) + \alpha(-1)^b \pi(n),\ n = 1, 2, ..., N_0, \quad (4)$$

где: $C_w(n)$ – контейнер с вложенной информацией;

$\alpha \in R$ – коэффициент глубины вложения;

$b \in \{0,1\}$ – значение вкладываемого бита;

$\pi(n)$ – псевдослучайная последовательность, задаваемая по стегоключу; обычно $\pi(n) \in \{+1,-1\}$ или $\pi(n) \in qN(0,1)$,

где: $qN(0,1)$ означает квантованную последовательность гауссовских отсчетов с нулевым средним и дисперсией «1».

Для разработки новых методов, как стеговложения так и стегоатак, необходимо понимать, какие именно методы стеговложения распространены на сегодняшний день и какие медиафайлы используются в качестве контейнеров. Эти данные позволят сформировать требования к новым методам стеговложений (или какие модификации необходимо провести с уже существующими методами).

При разработке новых методов стеговложений можно пойти двумя путями:

- выбрать наиболее распространенные, как контейнеры медиафайлы (поскольку пользователи к ним уже привыкли) и разрабатывать алгоритмы вложения для данных файлов;
- выбрать малоиспользуемые, как контейнеры медиафайлы, поскольку такие файлы при передаче вызовут меньше подозрений, и стегоатак для таких файлов существует, как правило, не много.

При разработке алгоритмов стегоатак особенно важно знать, какие именно методы вложения распространены на сегодняшний день. В настоящее время большинство стегоатак являются атаками «направленного действия». Другими словами, каждый конкретный алгоритм атаки разработан для выявления вложения, сделанного определенным методом (или схожей по свойствам группой методов) стеганографии. Поэтому, зная широко распространенные алгоритмы вложения, можно разработать стегоатаки, которые найдут широкое применение в современном мире.

Также для разработки стегоатак важно знать, какие именно медиафайлы чаще всего используются в качестве контейнеров при передаче скрытой информации. Стоит учесть, что большинство стегоатак направлено на выявления различных статистических свойств медиафайла с вложением и их отклонения от свойств чистого файла (файла, в котором нет вложения).

Медиафайлы разных форматов обладают разными статистическими свойствами. И хотя точные данные о статистических распределениях различных форматов медиафайлов на

сегодняшний день собрать невозможно, поскольку статистика компьютерных файлов достаточно сложна, все же алгоритмы стегоатак опираются на некие аппроксимированные свойства медиафайлов. Зная, какого именно формата файлы могут быть использованы в качестве контейнера можно разработать автоматизированные методы стегоатак для выявления медиафайлов с вложениями в большом потоке информации.

Сегодня в сети интернет можно найти программное обеспечение, которое позволяет вложить скрываемую информацию в различные медиафайлы. Часть этих программ является профессиональными, используемыми для защиты коммерческой тайны, личных данных и в других целям. Но есть и достаточное количество программ, которые распространяются свободно и не требуют от пользователя каких-либо специальных знаний и умений в области стеганографии. Нужно будет всего лишь нажать несколько кнопок в программе и получить медиафайл с вложенным в него скрытым сообщением. Отметим, что многие программные продукты распространяются бесплатно. Следовательно, методы передачи информации с использование методов стеганографии стали доступны достаточно большому числу людей – всем пользователям сети интернет.

Рассмотрим наиболее распространенное на сегодняшний день программное обеспечение, реализующее методы стеганографии:

- *Anubis* – программа 2014, в качестве контейнеров используются медиафайлы формата *BMP*. В качестве скрываемой информации – текстовый файл. Скрываемая информация дописывается в конец файла. Обнаружение такого рода вложений вычисляются элементарно;
- *DeEgger Embedder* – в качестве контейнеров используются медиафайлы форматов *BMP, PNG, JPG, AVI, MP3*. Скрываемая информация, как и в предыдущем случае, дописывается в конец файла. Такое вложение также очень легко выявить;
- *DeepSound* – в качестве исходных контейнеров используются файлы формата *WAV* (только несжатый, *PCM*), *MP3, CDA, WMA, APE, FLAC*, при этом на выходе, после внедрения информации, могут получиться файлы только форматов *WAV, APE, FLAC*. Для вложения информации в данной программе используется алгоритм вложения ШПС. Данная программа позволяет предварительно зашифровать скрываемую информацию криптографическим алгоритмом *AES*;
- *Hallucinate* – в качестве контейнеров используются файлы формата *BMP, PNG*. В качестве стенографического алгоритма используется алгоритм НЗБ;
- *JHide* – в качестве контейнеров используются файлы формата *BMP, PNG, TIFF*. В качестве стенографического алгоритма используется алгоритм НЗБ;
- *OpenPuff* – в качестве контейнеров используются медиафайлы с неподвижными картинками, видеопотоком или аудиозаписями (например, *MP4, MPG, VOB*). В качестве стенографического алгоритма используется алгоритм НЗБ. Скрываемая информация также защищается криптографическим стойким генератором псевдослучайных чисел (*CSPRNG – Cryptographically secure pseudorandom number generator*);
- *OpenStego* – в качестве исходных контейнеров используются файлы формата *MP, PNG, JPG, GIF, WBMP*. Есть возможность использования шифрования типа *AES*;
- *QuickStego* – в качестве исходных контейнеров используются файлы формата *BMP, JPG, GIF*, при этом на выходе, после внедрения информации, могут получиться файлы только формата *BMP*. В платной версии программы возможно использовать файлы формата *WAV, MP3*. В качестве стенографического алгоритма используется алгоритм НЗБ;
- *Xiao Steganography* – в качестве контейнеров используются файлы формата *BMP, WAV*. Данная программа также позволяет предварительно зашифровать скрываемую информацию криптографическими алгоритмами *RC4, Triple DES, DES, Triple DES 112, RC2* и алгоритмами хэширования *SHA, MD4, MD2, MD5*;

- *SilentEye* – в качестве контейнеров используются файлы формата *BMP, JPG, PNG, GIF, TIF, WAV*. Для шифрования вкладываемой информации криптографическими методами используется алгоритм *AES;*
- *Steghid*e – в качестве контейнеров используются файлы формата *JPG, BMP, WAV* и *AU*. В качестве стенографического алгоритма используется алгоритм НЗБ;
- *SSuite Picsel Security* – в качестве контейнеров используются файлы формата *BMP, JPG, WMF, PNG;*
- *StegoStick (beta*) – в качестве контейнеров используются файлы формата *JPG, BMP, GIF, WAV, AVI, PDF, EXE, CHM*. Для шифрования вкладываемой информации криптографическими методами используются алгоритмы *DES, Triple DES, RSA*;
- *Trojan* – в качестве исходных контейнеров используются файлы формата *JPG, BMP, TIF, GIF, PNG, MNG, PCS, TGA*, при этом на выходе, после внедрения информации, могут получиться файлы только форматов *BMP, PNG, TIF*;
- *SecurEngine Professional* 1.0 – в качестве контейнеров используются файлы формата *BMP, GIF, PNG, HTM*. Для шифрования вкладываемой информации криптографическими методами используются алгоритмы *AES, Gost, BlowFish, ThreeDe;*
- *bmpPacker 1.2a* – в качестве контейнеров используются файлы только формата *BMP*. Для шифрования вкладываемой информации криптографическими методами используются алгоритмы *AES, BlowFish, TwoFish;*
- *MP3Stego* 1.1.16 – в качестве контейнеров используются файлы только формата *MP3;*
- *Hide and Seek* 5.0 – в качестве контейнеров используются файлы только формата *GIF*. Для шифрования вкладываемой информации криптографическими методами используется алгоритм *BlowFish;*
- *Hide'N'Send* – в качестве контейнеров используются файлы только формата *JPEG*. В качестве стенографических алгоритмов используются алгоритмы НЗБ и *F5*. Для шифрования вкладываемой информации криптографическими методами используются алгоритмы *AES, RC4, RC2;*
- *S-Tools* – в качестве контейнеров используются файлы с неподвижными изображениями или звуком. Для шифрования вкладываемой информации криптографическими методами используются алгоритмы *DES, Triple DES и IDEA;*
- *Jsteg* – в качестве контейнеров используются файлы формата *JPG*. В качестве стенографического алгоритма используется алгоритм НЗБ;
- *StegoDos* – в качестве контейнеров используются файлы с неподвижными изображениями;
- Steganos – в качестве контейнеров используются файлы формата *BMP, DIB, VOC, WAV, ASCII, HTML*. Для шифрования вкладываемой информации криптографическими методами используется алгоритм *AES*;
- *DarkJPEG* – в качестве контейнеров используются файлы формата *JPEG*. Для шифрования вкладываемой информации криптографическими методами используется алгоритм *AES;*
- *FFEncode* – в качестве контейнеров используются текстовые файлы.

Проанализировав как программное обеспечение, приведенное выше, так и другие программные продукты, использующие алгоритмы стеганографии, можно сделать вывод, что наиболее часто в качестве контейнеров для вложения используются медиафайлы с неподвижными изображениями. Существует несколько причин популярности именно изображений в качестве контейнеров для стеговложений.

Во-первых, это распространенность данного типа медиафайлов. Изображения (картинки, фотографии и т.д.) в настоящее время очень популярны в сети интернет, их можно встретить практически на всех *web*-страницах, существующих сегодня в глобальной сети. При этом на сегодняшний день в сети интернет получили широкое распространение социальные сети, куда миллионы пользователей каждый день добавляют новые изображения, как на свои персональные

страницы, так и в группы пользователей. Другими словами, обмен, размещение на сайтах и другой способ передачи неподвижных изображений между пользователями сети интернет не вызывает ни у кого подозрений. К тому же в таком потоке однородной информации сложно заметить медиафайл, даже если он и может вызвать подозрение, а значит неподвижное изображение с вложенной в него информацией легко «спрятать» от посторонних глаз на самом видном месте – в сети интернет.

Во-вторых, широко распространенные на сегодняшний день алгоритмы вложения в неподвижные изображения достаточно просты в реализации. Многие из современных методов стеганографии, используемых для вложения информации в неподвижные изображения, не требуют ни сложных вычислений, ни больших вычислительных мощностей. Это позволяет использовать данные алгоритмы на обычных домашних компьютерах, не обладающих большими ресурсами.

В-третьих, неподвижные изображения – как «невинные», так и изображения со стеговложениями, – имеют сложную статистику. Статистика неподвижных изображений (как и многих других медиафайлов) на сегодняшний день известна не полностью. Данный факт влияет как на разработку современных стегосистем, так и на разработку стегоатак. Не зная предполагаемых статистических свойств контейнера сложно разработать, не только надежные методы вложения информации, но и эффективные методы выявления стеговложений. Сложность реализации атак также является преимуществом использования в качестве контейнеров неподвижных изображений.

Самым часто используемым стеганографическим алгоритмом в рассмотренных программных продуктах является алгоритм вложения в НЗБ и его модификации. Методы, основанные на вложении в НЗБ, как правило, хорошо подходят для вложения информации в неподвижные изображения. Преимуществом большинства методов, основанных на вложении в НЗБ, является простота реализации, которая обычно не требует выполнения сложных вычислений.

Основным недостатком методов вложения в НЗБ можно назвать неустойчивость к специально разработанным для данных алгоритмов стегоатакам. Они позволяют достаточно надежно определить наличие или отсутствие вложения в неподвижном изображении. И хотя методы вложения в НЗБ постоянно совершенствуются, становясь устойчивыми к уже существующим стегоатакам, постоянно разрабатываются новые методы выявления вложений для новых алгоритмов стеганографии. Но стоит заметить, что при правильном использовании существующих методов вложения в НЗБ (выбор метода вложения с учетом статистических особенностей контейнера, вложения малого объема информации, чтобы изменение статистических свойств исходного медиафайла незначительно менялись после вложения и эти изменения невозможно было отследить) определить наличие или отсутствие вложения даже с помощью стегоатак достаточно сложно.

Обладая информацией, какие именно медиафайлы чаще всего используются в качестве контейнера и какие именно методы стеганографии применяются для вложения, можно сделать выводы, какие методы стеговложений и стегоатак требуется разрабатывать.

Заключение

Данные сведения могут найти практическое применение в государственных структурах как для организации, так и для обнаружения скрытых каналов передачи данных между террористами и другими криминальными группировками, а также в бизнесе для обнаружения и противодействия промышленному шпионажу.

Литература

1. Betancourt S.R. Steganography: A New Age of Terrorism [Электронный ресурс] / S.R. Betancourt // SANS Institute, 2004. – 10 с.

– Режим доступа: http://www.giac.org/paper/gsec/3494/steganography-age-terrorism/102620 (Дата обращения 10.10.2019).
2. Fridrich, Jessica. Steganography in Digital Media Principles, Algorithms and Applications / Jessica Fridrich. – Campridge University Press, 2010. – P. 462.
3. Коржик В.И. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография: [монография] / В.И. Коржик, К.А. Небаева, Е.Ю. Герлинг, П.С. Догиль, И.А. Федянин; под общ. ред. проф. В.И. Коржика; СПбГУТ. – СПб.: 2016 – 226 с.
4. Герлинг Е.Ю. Исследование и разработка методов обнаружения стеговложений в неподвижных изобаржений: Дис. канд. техн. наук: 05.12.13; [Место защиты: СПбГУТ]. – СПб.: 2014. – 211 с.
5. Коржик В.И. Обнаружение видеостегосистем при вложении секретной информации в наименьшие значащие биты / В.И. Коржик, Е.Ю. Герлинг, А.П. Дубов // Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Юбилейная научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов, 57-я. 24-28 января 2005 года: материалы. – СПб.: СПбГУТ. – 2005. – С. 148-149.
6. Conway, M. Code Wars: Steganography, Signals Intelligence, and Terrorism. Knowledge, Technology and Policy / M. Conway // Special issue entitled Technology and Terrorism, 2003. – Vol. 16, – №. 2. – p. 45-62.
7. Коржик В.И. Построение стегосистемы, инвариантной к статистике покрывающего сообщения / В. И. Коржик, Е. Ю. Герлинг // Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов, 59-я. 22-26 января 2007 года: материалы. – СПб.:СПбГУТ, 2007. – С. 184-185.
8. Ker, A. Steganalysis of LSB Matching in Grayscale Images / A. Ker // Signal Processing Letters. – 2005. – Vol. 12. – Pp. 441-444.
9. Коржик В.И. Построение идеально стойкой лингвистической стегосистемы с редактируемым текстом / В.И. Коржик, А.А. Залетов // Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов, 60-я. 21-25 января 2008 года: материалы. – СПб.: СПбГУТ, 2008. – С. 168.
10. Герлинг Е.Ю. Исследование эффективности методов обнаружения стегосистем, использующих широкополосное вложение / Е.Ю. Герлинг // Телекоммуникации, 2014. – № 1. – С. 6-12.
11. Ахрамеева К.А. Возможность удаления, предполагаемого стеговложения в цифровых видеопоследовательностях с использованием линейной коллизии вложение / К.А. Ахрамеева, Л.Г. Попов // Телекоммуникации, 2018. – № 4. – С. 18-24
12. Pevny, T.Towards Multi-class Blind Steganalyzer for JPEG Images / T. Pevny, J. Fridrich // Lecture Notes in Computer Science, 2005. – Vol. 3710. – p. 39-53.
13. Fridrich, J. Feature-Based Steganalysis for JPEG Image and its Implication for Future Design of Steganographic Schemes / J. Fridrich // Lecture Notes in Computer Science, 2005. – Vol. 3200. – p. 67-81.
14. Lee, Y.-K. An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding / Y.-K. Lee, G. Bell, S.-Y. Huang, R.-Z. Wang, S.-J. Shyu // Lecture Notes in Computer Science, 2009. – Vol. 5414. – Pp. 349-360.
15. Герлинг Е.Ю. Исследование эффективности методов обнаружения стегосистем, использующих вложение в наименее значащие биты / Е.Ю. Герлинг // Информационные системы и технологии, 2011. – № 4. – С. 137-144.

16. Das, S. Steganography and Steganalysis: Different Approaches [Электронный ресурс] / S. Das, S. Das, B. Bandyopadhyay, S. Sanyal // International Journal of Computers, Information Technology and Engineering. – 2008. – Vol. 2. – Режим доступа: http://arxiv.org/ftp/arxiv/papers/1111/1111.3758.pdf (Дата обращения 06.10.219).
17. Jesse, D.D. Tactical Means, Strategic Ends: Al Qaeda's Use of Denial and Deception / D.D. Jesse // Terrorism and Political Violence, 2006. – Vol. 18. – p. 367-388.
18. Ахрамеева К.А. Анализ методов анализа цифровых видеопоследовательностей. вложение / К.А. Ахрамеева, Л.Г. Попов // Телекоммуникации, 2017. – № 1. – С. 33-40.
19. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-ПРЕСС, 2009. – 265 с.