BIBLIOGRAPHIC LIST

1. *Shannon C.E.* Communication Theory of Secrecy Systems // Bell Syst. Tech. Journal. – 1949. – Vol. 28.
2. FIPS 46-3. Data Encryption Standard (DES).
3. *Biryukov D.*Wagner. Slide Attacks. Proceedings of FSE'99, LNCS 1636. Springer Verlag. 1999. – P. 245-259.
4. *Biham E.* New Types of Cryptanalytic Attacks Using Related Keys // Journal of Cryptology. – 1994. – Vol. 7. – P. 229-246.
5. Announcing development of a federal information processing standard for Advanced Encryption Standard. Department of Commerce. National Institute of Standards and Technology, USA. 1997. Available at http://csrc.nist.gov/archive/aes/pre-round1/aes_9701.txt.
6. New European Schemes for Signature, Integrity, and Encryption. Call for Cryptographic Primitives. Information Societies Technology (IST) Program of the European Commission, 2000. Available at https://www.cosic.esat.kuleuven.be/nessie/call.
7. *Daemen J., Rijmen V.* The design of Rijndael. AES –The Advanced Encryption Standard. Springer-Verlag, Berlin. 2002.
8. *Courtois N.T., Pieprzyk J.* Cryptanalysis of block ciphers with overdefined systems of equations. Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, 2002.

Олейников Роман Васильевич
ЗАО «Институт информационных технологий».
E-mail: ROliynykov@gmail.com.
Украина, 61166, г. Харьков, ул. Бакулина, 12.
Тел.: +380577142205; +380675733343.

Руженцев Виктор Игоревич
E-mail: vityazik@rambler.ru.

Oliynykov Roman Vasil'evich
JSC "Institute of Information Technologies".
E-mail: ROliynykov@gmail.com.
12, Bakulina street, Kharkov, 61166, Ukraine.
Phone: +380577142205; +380675733343.

Ruzhentsev Viktor Igorevich
E-mail: vityazik@rambler.ru.

УДК 003.26

А.Т. Алиев

ЛИНГВИСТИЧЕСКАЯ СТЕГАНОГРАФИЯ НА ОСНОВЕ ЗАМЕНЫ СИНОНИМОВ ДЛЯ ТЕКСТОВ НА РУССКОМ ЯЗЫКЕ

Рассматриваются методы скрытой передачи информации, основанные на использовании синонимов. Основной задачей является исследование возможности реализации данных методов для текстов на русском языке. Для этого в работе был проведен анализ особенностей русского языка и его частотных свойств, построены специальные словари синонимов для разных частей речи и предложены новые алгоритмы сокрытия и извлечения информации.

Сокрытие информации; скрытая передача информации; стеганография; лингвистическая стеганография; текст; метод синонимичных преобразований; синонимичная замена.

A.T. Aliev

LINGUISTIC STEGANOGRAPHY METHODS BASED ON THE SYNONYMOUS SUBSTITUTION FOR TEXTS IN RUSSIAN

In this paper we consider methods of secure communication based on the synonymous substitution. The main task is to research the feasibility of use of these methods to texts in Russian. We analyzed the features of the Russian language and its frequency, built special dictionaries of synonyms for different parts of speech and proposed new algorithms for hiding and retrieving information.

Information hiding; secure communication; steganography; linguistic steganography; the text; the method of synonymous changes; synonymous substitution.

В последние годы отчетливо прослеживается рост интереса к стеганографическим методам защиты информации. Появляется все больше новых интересных методов и алгоритмов, совершенствуются старые. Анализ публикаций, представленных в открытой печати, позволяет говорить о том, что подавляющее большинство исследований, новых методов и решений ориентировано на работу и использование в качестве контейнеров мультимедиа информации, такой как изображения, оцифрованный аудиосигнал, видео. Прогресс в области новых методов стеганографии и стеганоанализа в данном направлении очевиден. В то же время нельзя забывать о том, что огромное количество информации представлено в обычном текстовом виде: книги, статьи, электронная переписка, документы, отчеты и многое другое. Все эти материалы также могут быть эффективно использованы в качестве контейнеров для скрытой передачи информации.

Актуальность проблемы. Методам скрытой передачи информации в текстовых документах посвящено такое направление в технологиях скрытой передачи информации как лингвистическая стеганография. Отличительной особенностью данного направления является то, что в качестве контейнеров используются обычные открытые тексты. То есть те тексты, которые мы с вами читаем и составляем каждый день. Конечно, объем информации, которую можно скрыто передать с использованием методов лингвистической стеганографии невелик, если сравнивать с методами, использующими мультимедиа контейнеры. Но так ли часто нужно скрыто передавать мегабайты информации? Порой достаточно и нескольких слов или предложений. И в этом случае лингвистической стеганографии нет равных, так как скрытое послание может быть отправлено адресату как угодно, например, хоть по электронной, хоть по обычной почте. Оно даже может быть зачитано вслух или продиктовано по телефону. Стеганографические же методы, работающие с мультимедиа контейнерами, в большинстве случаев оказываются нестойкими даже в случае простого сохранения документа-контейнера в другом формате.

Постановка задачи. Рассматривая работы зарубежных специалистов, посвященные лингвистической стеганографии, как например [1, 2, 3], можно заметить, что авторы этих работ достаточно четко разграничивают методы и алгоритмы лингвистической стеганографии по защите скрываемой информации от «роботов» (программ автоматического сканирования и анализа текстов) и от людей. Первые направлены на защиту информации при тотальном сканировании всей корреспонденции программными поисковыми роботами. Вторые направлены на защиту информации при внимательном просмотре текста человеком. Не вызывает удивления тот факт, что публикаций и работ, посвященных первому направлению на порядок больше работ, посвященных второму направлению (защите от анализа человеком). Поисковые роботы ищут ключевые слова, фразы, какие-то явные особенности текста. В результате, робота, который не силен в грамматике и не пони-

мает смысла и явного подтекста передаваемых сообщений, обмануть гораздо проще. Задача же скрытой передачи информации в тексте, нацеленная на защиту от анализа передаваемого сообщения человеком, очевидно на порядок сложнее.

В данной работе была поставлена задача: разработать и реализовать методы скрытой передачи коротких сообщений, использующие в качестве контейнеров тексты на русском языке и при этом обеспечить защиту как от визуального анализа, проводимого человеком, так и от статистического анализа, который может быть проведен роботами.

Решить поставленную задачу для текстов на русском языке в действительности значительно сложнее, нежели для текстов на английском языке. Здесь можно выделить два основных фактора, приводящих к усложнению задачи. Первым из них является неоднозначное использование слов в русском языке. В различном контексте одни и те же слова могут нести совершенно различную смысловую нагрузку. Вторым фактором является широкое использование в русском языке большого количества окончаний слов. Если при построении стеганографической системы не учитывать хотя бы один из этих факторов, результирующий текст будет носить явно несогласованный характер, что является очевидным демаскирующим признаком.

Метод замены синонимов. В качестве основы для разработки новых методов был взят метод лингвистической стеганографии, основанный на использовании синонимов. Принцип работы базового метода прост. Довольно часто в тексте одно слово может быть заменено другим словом, которое является синонимом исходного слова. В качестве примера можно привести два предложения, несущих одинаковую смысловую нагрузку: «На улице сейчас *прекрасная* погода» и «На улице сейчас *замечательная* погода». Так как предложения несут одинаковую смысловую нагрузку, то использование их в тексте эквивалентно. Для того чтобы передать скрытое сообщение первому предложению, мы можем поставить в соответствие двоичный «0», второму – двоичную «1» скрываемого сообщения.

Как видно из представленного примера, использование стеганографического метода, основанного на замене синонимов, позволяет сохранить синтаксическую структуру предложения и его смысловую нагрузку. Такую замену слов достаточно легко проделать человеку. В то же время этот метод нельзя реализовать простым машинным алгоритмом, даже если не учитывать необходимость подстановки окончаний и согласования слов. Можно заметить, что в русском языке существует достаточно большое количество пар {слово; синоним}. Использование всех таких пар для целей стеганографического сокрытия информации, когда слову ставится в соответствие двоичный «0», а его синониму «1» очередного бита скрываемого сообщения, часто приводит к значительным искажениям смысловой нагрузки скрывающего текста. Как следствие, из-за неправильного употребления синонимов текст, содержащий скрытую информацию, становится легко идентифицируемым, и, в свою очередь, позволяет противнику установить наличие скрытого сообщения.

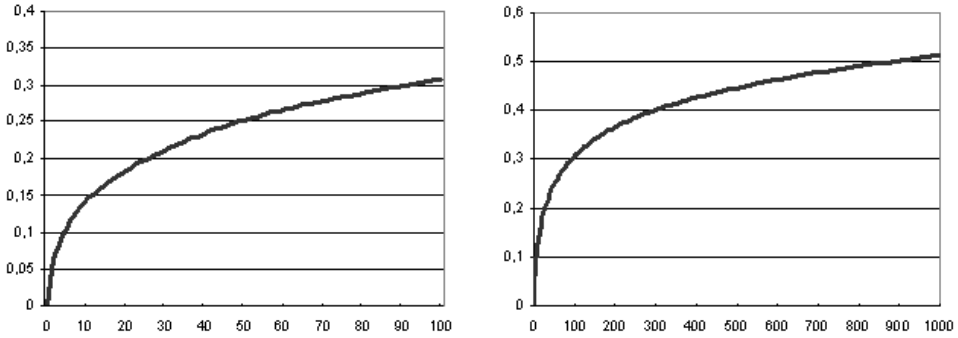
Тут мы сталкиваемся с противоречием. Требование максимизации пропускной способности для метода скрытой передачи информации на основе замены синонимов, на первый взгляд, явным образом требует использования максимально большого словаря синонимов. Очевидно, что чем больше слов в используемом словаре синонимов, тем большее количество слов в тексте можно будет заменить и использовать для записи информации. Но чем больше слов в словаре синонимов, тем выше вероятность их неправильного употребления. Например, два слова «машина» и «автомобиль» являются синонимами, но в предложении «Новая стиральная машина» синоним «автомобиль» использовать нельзя.

Причина невозможности замены слова синонимом в приведенном выше примере объясняется тем, что мы столкнулись с неоднозначными синонимами, использовать которые можно только в зависимости от контекста. В действительности в русском языке можно выделить два класса синонимов: однозначные и неоднозначные. Первые могут быть использованы в любом контексте, вторые только в определенном смысловом значении. На первый взгляд лучшим решением было бы отказаться от использования неоднозначных синонимов и использовать для целей скрытой передачи информации только однозначные синонимы. Но такое решение приведет к сильному снижению информационной емкости контейнеров, так как однозначные синонимы составляют малую часть множества всех возможных синонимов. Компромисс все же может быть найден. Здесь следует отметить тот факт, что довольно большую группу синонимов составляют синонимы, употребление которых в несвойственном им контексте маловероятно. Включение таких синонимов в словарь позволяет значительно увеличить информационную емкость при относительно небольшом проценте неверных замен.

Ограничение словаря синонимов. В целях сведения к минимуму числа неконтролируемых замен синонимов вместо полного словаря синонимов для русского языка, как например [4], предлагается использовать ограниченный словарь, состоящий только из наиболее часто употребляемых слов. С целью оптимизации размера словаря синонимов был проведен анализ большого количества русскоязычных текстов различных стилей, жанров и направлений [5]. Для проведения анализа была подготовлена база текстов, содержащая более 14 тысяч произведений различных жанров и направлений на русском языке. Все файлы базы были переведены в простой текстовый формат, при этом общий объем базы составил порядка 8 Гб (один символ текста – один байт). Для обработки такого объема текстовой информации потребовалось задействовать вычислительный кластер из десяти машин, при этом время обработки данных составило около одной недели. В результате, благодаря высокой репрезентативности текстовой базы, были получены достоверные данные о частотах встречаемости слов русского языка.

Вполне очевидно, что встречаемость слов в текстах на русском языке является неравномерной, и можно выделить как часто, так и редко употребляемые слова. Но проведенный анализ полученных результатов позволил все же сделать неожиданное заключение. Как оказалось, первые сто наиболее часто употребляемых слов в совокупности обеспечивают покрытие более 30 % какого-либо осмысленного текста и наблюдается обратная экспоненциальная зависимость покрытия текста от объема словаря. Словарь из 300 наиболее часто употребляемых слов обеспечивает покрытие порядка 40 %, а словарь из 1000 слов обеспечивает покрытие чуть более 50 % любого осмысленного текста. Соответствующие графики степени покрытия осмысленных текстов для словарей, содержащих первые сто и тысячу наиболее часто употребляемых слов, представлены на рис. 1.

Учитывая представленные результаты, можно говорить о том, что словарь синонимов для стеганографического метода синонимичных преобразований может быть существенно ограничен без серьезной потери в информационной емкости. Если ограничить словарь синонимов только наиболее часто употребляемыми словами, то его будет гораздо легче грамотно обработать. В данном случае небольшая потеря в информационной емкости метода позволяет значительно улучшить его скрытность, которая непосредственно связана с качеством используемого словаря синонимов. Уменьшая размер словаря, мы тем самым предоставляем возможность для его внимательной проработки, которая, в свою очередь, позволит исключить использование редко употребляемых слов в несвойственном им контексте. В результате можно значительно снизить вероятность замены исходных слов в тексте синонимами с неподходящим для данного контекста значением.



а б

Рис. 1. Покрытие текстов первой сотней (а) и первой тысячей (б) наиболее часто употребляемых слов

Формирование и формат словарей синонимов. В русском языке слова довольно редко употребляются без соответствующих окончаний, позволяющих согласовать данное слово с его окружением в тексте. Данный факт необходимо учитывать при формировании словаря синонимов. Ведь практически любая замена слова, произведенная без учета его окончания, может привести к разрушению структуры предложения, что легко обнаружить. Следовательно, алгоритм сокрытия информации, работающий с русскоязычными текстами, при замене одних слов другими, непременно должен учитывать окончания этих слов. Здесь нужно особо отметить, что простая подстановка окончания исходного слова к заменяющему его слову не приведет к желаемому результату, так как даже существительные в одном и том же падеже могут иметь разные окончания. Кроме того, различные части речи используют различные механизмы словообразования.

Для решения этой проблемы предлагается разбить словарь синонимов на отдельные таблицы в соответствии с частями речи: существительные, прилагательные, числительные, местоимения, глаголы, наречия, предлоги, союзы, частицы и связки. Помимо самих слов, в таблицы заносятся и все возможные окончания в соответствии с падежом, родом, числом, склонением и спряжением. Эти окончания выписываются последовательно для каждого слова в отдельности. Если окончание отсутствует, то соответствующее поле остается пустым, но список через запятую продолжается дальше. В результате для каждого слова из словаря синонимов в первом приближении формируется список, состоящий из слов и всех возможных окончаний. Формат записей в словаре синонимов первого приближения представлен на рис. 2.

<v> (<e1>, <e2>, …), <s1> (<e1>, <e2>, …), …

<v> - слово;
<s#> - синоним;
<e#> - окончание слова или синонима.

Рис. 2. Формат словаря синонимов первого приближения

К недостаткам словарей синонимов первого приближения можно отнести тот факт, что в случае отсутствия окончания у исходного слова более чем в одной позиции или наличия двух и более одинаковых окончаний, становится невозможным точно подобрать окончание для замещающего его слова. Выбрать нужное оконча-

ние можно, если посмотреть в каком контексте употребляется исходное слово. Однако данную операцию не так легко реализовать программно. Вместо рассмотрения слов, входящих в окружение заменяемого слова, предлагается опереться только на окончания соседних слов. Окончания слов предшествующего или следующего за заменяемым словом в большинстве случаев позволяют легко определить в каком падеже, числе или склонении употребляется заменяемое слово и в соответствии с этим подставить нужное окончание к замещающему слову. Таким образом, в качестве второго приближения предлагается ввести учет окончаний слов слева и справа от заменяемого слова. В этом случае, помимо окончаний самого заменяемого слова и его синонимов, в список заносятся все возможные окончания для слов слева и справа от данного слова. Формат отдельной записи для словарей второго приближения представлен на рис. 3.

<v> (<e1> (<l1>, <l2>, … : <r1>, <r2>, …), <e2> (<l1>, <l2>, … : <r1>, <r2>, …), …),
<s> (<e1> (<l1>, <l2>, … : <r1>, <r2>, …), <e2> (<l1>, <l2>, … : <r1>, <r2>, …), …),
…

<l#> - окончание слова слева от данного слова;
<r#> - окончание слова стоящего справа от данного слова.

Рис. 3. Формат словаря синонимов второго приближения

Использование словарей второго приближения позволяет повысить точность согласования замещающих слов и снизить вероятность неправильного употребления окончаний у замещающих слов к минимуму. Однако формирование словарей второго приближения и реализация соответствующего метода сокрытия информации является более сложной задачей, нежели использование словарей первого приближения. При этом, как показали результаты экспериментов, в большинстве случаев можно ограничиться словарями первого приближения. Возможные огрехи в выборе окончаний можно исправить после сокрытия информации, просмотрев и отредактировав итоговый текст вручную.

Простой алгоритм сокрытия информации в текстовых данных. В простом варианте реализации алгоритма замена слов осуществляется без учета статистических данных. Он основан на простом методе замены слов. В этом случае вектор синонимов для каждого слова из словаря синонимов нормируется по длине, которая должна быть кратной степени двойки. В случае, если длина вектора синонимов оказывается больше необходимой, то из него удаляются наиболее редко используемые синонимы. Количество битов скрываемой информации t для каждого слова определяется исходя из длины l вектора синонимов: $t = log_2 l$. Каждому из синонимов в векторе ставится в соответствие двоичное представление числа из диапазона 0, …, $2^t - 1$. В процессе записи информации из очередного вектора синонимов выбирается слово, двоичное представление номера которого соответствует текущему двоичному вектору скрываемой информации длины t. Выбранное слово и становится заменой текущего слова. После того, как очередное замещающее слово было выбрано, оно вставляется в текст на место исходного слова с использованием соответствующего окончания.

Алгоритм учитывающий частоты употребления слов. Важно отметить, что применение простого метода замены слов можно считать приемлемым только в случае использования коротких текстовых сообщений. Использование данного метода для относительно больших текстов приведет к возможности обнаружения скрытого канала методами статистического анализа. Так если скрываемые данные будут представлять собой двоичные последовательности с равномерным распре-

делением, то на выходе частоты слов могут сильно измениться. Редко употребляемые в обычных текстах слова будут использоваться наравне с наиболее часто употребляемыми словами.

Для сохранения частотных характеристик текстов предлагается дополнить словарь синонимов дополнительной таблицей частот встречаемости слов, входящих в словарь синонимов. Также необходимо изменить и сам алгоритм сокрытия информации. Для начала рассмотрим случай, когда словарь синонимов содержит записи S_k, состоящие только из двух слов S^k_1 и S^k_2 (слово и один его синоним), отдельная запись имеет вид $S_k = \{S^k_1, S^k_2\}$. Вероятность появления слов S^k_1 и S^k_2 в осмысленном тексте на русском языке p_i и p_j соответственно. Нормируем вероятности таким образом, чтобы $z\cdot(p_i + p_j) = 1$. Пусть $R \in [0, 1)$ – случайное число.

Положим, что в ходе выполнения процедуры сокрытия информации обнаружено слово, принадлежащее S_k. Тогда если $R \in [0, z\cdot p_i)$ в качестве замещающего слова выбирается слово S следующим образом:

$$S = \begin{cases} S^k_1 : bit = 0 \wedge R \in [0, z\cdot p_i) \\ S^k_2 : bit = 1 \wedge R \in [0, z\cdot p_i) \\ S^k_1 : bit = 0 \wedge R \in [z\cdot p_i, 1) \\ S^k_2 : bit = 1 \wedge R \in [z\cdot p_i, 1) \end{cases}$$

В общем случае множества записей S_k могут состоять из двух и более слов. Для упрощения алгоритмической реализации положим, что число слов в записи S_k кратно степени двойки. Обозначим число слов в записи с индексом k через N_k. Разобьем интервал [0, 1) на N_k непересекающихся отрезков, в соответствии с частотами слов, входящих в запись S_k. Тогда при выборе слова из S_k по случайному числу R определяется номер t отрезка, в который попадает значение числа R. Далее определяется номер слова в записи S_k как $t' = (t + dat) \bmod N_k$, где dat – десятичное представление очередных $log_2(N_k)$ бит скрываемых данных. В качестве замещающего слова выбирается слово $S^k_{t'}$.

В результате использования предложенной модификации метода одно и то же слово в разных частях текста может кодировать различные скрываемые данные. При этом частоты появления слов в конечном тексте будут близки к частотам встречаемости этих слов в любых других текстах, что делает невозможным проведение атаки методом частотного анализа. Ограничением данной модификации является необходимость синхронизации генераторов псевдослучайных чисел на стороне отправителя и на стороне получателя.

Необходимость синхронизации генераторов псевдослучайных чисел на стороне отправителя и получателя по сути вводит в систему стеганографический ключ – некоторую конечную последовательность данных, которая может быть использована для инициализации генераторов псевдослучайных чисел. Использование стеганографического ключа позволяет говорить о том, что только непосредственные участники информационного обмена (кому известен стеганографический ключ) могут извлечь передаваемую информацию.

Интересно также отметить, что использование таблицы частот встречаемости слов позволяет оценить информационную емкость стеганографического метода синонимичных замен, основанного на том или ином словаре синонимов как:

$$I = \sum_k log_2(N_k) \sum_{S^k} p_i \, .$$

Общая схема системы встраивания информации в текстовые данные. Вне зависимости от использования словарей синонимов первого и второго приближения, а также соответствующих им алгоритмов сокрытия информации можно предложить общую схему системы сокрытия информации в текстовых данных. Предлагаемая схема представлена на рис. 4. Входными данными являются: исходный текст, который используется в качестве контейнера для передачи скрытого сообщения; скрываемые данные – короткая двоичная последовательность; ключ – секретный параметр стеганографической системы. На выходе формируется итоговый текст, содержащий скрытое сообщение.

С целью обеспечения возможности реализации описанных выше стеганографических методов в схему системы дополнительно включены генератор псевдослучайной последовательности (ПСП) и таблица частот встречаемости слов в русском языке, содержащая только частоты для слов из словаря синонимов. В этом случае в процессе записи используется алгоритм, который в зависимости от данных генератора случайных чисел, скрываемых данных и частот встречаемости слов в естественных текстах осуществляет подстановку соответствующих синонимов. Стеганографический ключ в данном случае используется только для инициализации генератора псевдослучайных последовательностей. Использование ключей в качестве данных для инициализации генератора псевдослучайной последовательности позволяет обеспечить различный порядок замены слов для разных пользователей.

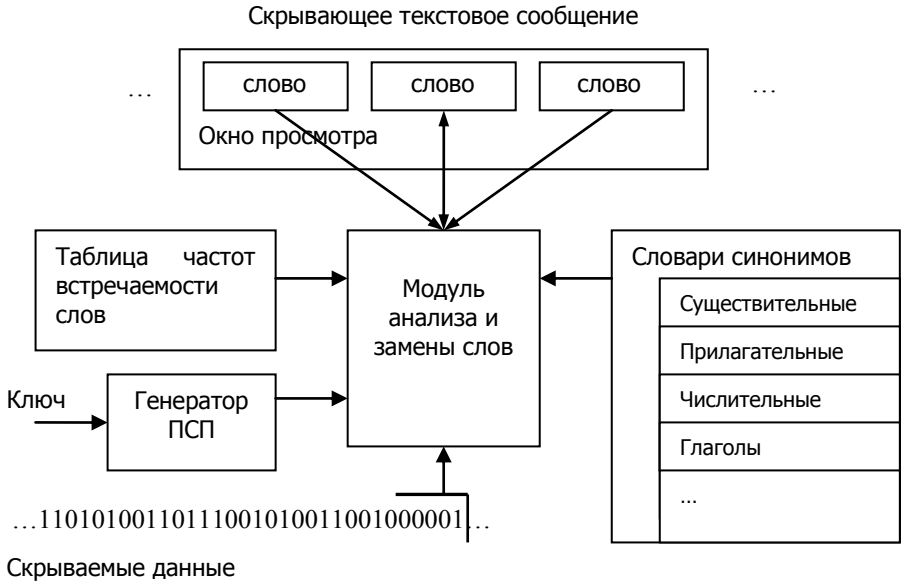


Рис. 4. Схема системы сокрытия информации в текстовых данных

Так как для сокрытия информации используются только слова, входящие в словарь синонимов, то предложенная схема позволяет обеспечить возможность предварительного анализа объема контейнера без учета скрываемой информации. За счет этого можно подобрать скрывающий текст из множества предварительно подготовленных документов под конкретное скрываемое сообщение. Это, в свою очередь, позволяет избежать использования контейнеров большой емкости для передачи коротких сообщений и гарантировать возможность записи в контейнер заранее определенного объема скрываемой информации. Таким образом, можно

рационально использовать заранее подготовленный набор текстовых документов и обеспечить работу всей системы в автоматическом режиме.

Апробация. Все представленные в работе методы и алгоритмы были апробированы и под них были написаны соответствующие программные реализации. Апробация предложенных алгоритмов позволяет говорить об их реальной эффективности. Так при встраивании сообщений в тексты объемом порядка нескольких страниц для метода, основанного на словарях первого приближения, приходилось исправлять только единичные слова и окончания, а не корректировать окончания у всех замененных слов. Особенностью реализации метода также является то, что уже измененные тексты, содержащие скрытые данные, можно свободно редактировать для лучшего согласования отдельных слов. Так, в конечной программной реализации, если редактирование не затрагивает слов из словаря синонимов, то никаких дополнительных действий после коррекции производить не требуется. Если же в процессе редактирования было принято решение заменить одно из слов синонимов другим словом или же вставить, или удалить кусок текста, то программа автоматически осуществляет перекодирование текста следующего за измененным участком с учетом внесенных пользователем изменений.

Заключение. В работе рассмотрены особенности реализации стеганографического метода на основе замены синонимов для текстов на русском языке. Предложены способы его улучшения и адаптации для работы с текстами на русском языке. Показана возможность существенного ограничения словарей синонимов без значительной потери в информационной емкости. Предложены новые методы сокрытия информации в текстовых данных, использующие специальные словари синонимов и частотные таблицы слов. Использование предложенных методов позволяет не только обеспечить возможность сокрытия информации в русскоязычных текстах в автоматическом режиме, но и обеспечить высокую скрытность передаваемых сообщений. Отличительной особенностью предложенных методов является возможность использования стеганографического ключа, данные которого непосредственно влияют на процесс сокрытия информации. Также представлена общая схема системы сокрытия информации и освещены алгоритмы, используемые при встраивании скрываемой информации.

Предложенные методы и алгоритмы могут быть использованы как для целей скрытой передачи информации, так и для целей защиты авторского права на текстовые произведения за счет их скрытой маркировки [6].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Bennett K.* Linguistic Steganography: survey, analysis, and robustness concerns for hiding information in text, Center for Education and Research in Information Assurance and Security, CERIAS Tech Report 2004-13. – 30 p.
2. *Calvo H., Bolshakov I. A.* Using selectional preferences for extending a synonymous paraphrasing method in steganography, Advances en Ciencias de la Computacion e Ingenieria de Computo - CIC'2004: XIII Congreso Internacional de Computacion, October 2004. – P. 231-242.
3. *Wayner P.*, Disappearing Cryptography – Information Hiding: Steganography & Watermarking, Morgan Kaufmann Publishers, Los Altos, CA 94022, USA, 2002. – 413 p.
4. *Абрамов Н.* Словарь русских синонимов и сходных по смыслу выражений. – М.: Русские словари, 1999.
5. *Алиев А.Т., Щербакова А.Н.* Анализ статистических свойств русского языка // Компьютерные технологии в науке, производстве, социальных и экономических процессах: Материалы X Междунар. науч.-практ. конф. – Новочеркасск: ЮРГТУ, 2009. – С. 55-58.
6. *Алиев А.Т.*, Защита электронных учебных пособий от нелегального распространения // Математические методы в технике и технологиях – ММТТ-22: Сборник трудов XXII Междунар. науч. конф.– Ростов-на-Дону: Издательский центр ДГТУ, 2009. – Т.11. – С. 127-135.

Алиев Александр Тофикович
Государственное образовательное учреждение высшего профессионального образования «Донской государственный технический университет».
E-mail: A.T.Aliev@mail.ru.
344000, г. Ростов-на-Дону, пл. Гагарина, 1.
Тел.: +79094205581.

Aliev Alexander Tofikovich
State educational institution of higher education “Don State Technical University”.
E-mail: A.T.Aliev@mail.ru.
1, Gagarin Square, Rostov-on-Don, 344000, Russia.
Phone: +79094205581.

УДК 004.056.55

А.Ф. Чипига

ОБОСНОВАНИЕ ВОЗМОЖНОСТИ СОХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В СИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧА ШИФРОВАНИЯ

Показана возможность сохранения конфиденциальности данных при компрометации ключа шифрования за счет использования энергетической и структурной скрытности сигналов на физическом уровне эталонной модели взаимосвязи открытых систем.

Информационная безопасность систем связи; энергетическая скрытность; структурная скрытность; информационная скрытность.

A.F. Chipiga

THE SUBSTANTIATION OF A POSSIBILITY TO MAINTAIN CONFIDENTIALITY IN SYMMETRIC CRYPTOSYSTEMS IN CASE OF A COMPROMISE OF AN ENCRYPTION KEY

The possibility of maintaining confidentiality in symmetric cryptosystems in case of a compromise of an encryption key using energetic and structural signal hiding on physical layer of OSI reference model was shown.

Information security of communications; energetic signal hiding; structural signal hiding; informational hiding.

Введение. Постановка задачи. Рост объемов конфиденциальной информации, передаваемой по незащищенным каналам связи, привел к широкому применению криптографических методов защиты. При этом предполагается, что криптография должна обеспечить такую защиту конфиденциальной информации, что даже в случае ее перехвата противником и обработки любыми способами с использованием современных и перспективных средств вычислительной техники она не должна быть дешифрована в течение нескольких десятилетий. Криптографическая стойкость системы шифрования должна определяться исключительно криптографической стойкостью ключа.

Проводимые мероприятия по противодействию угрозам безопасности информации приводят к значительному снижению возможности неправомерного овладения охраняемыми сведениями. Однако статистика говорит о том, что до