УДК 381.3

Разработка транслитерационного обратимого кодека для безопасной передачи информации по каналам связи общего пользования

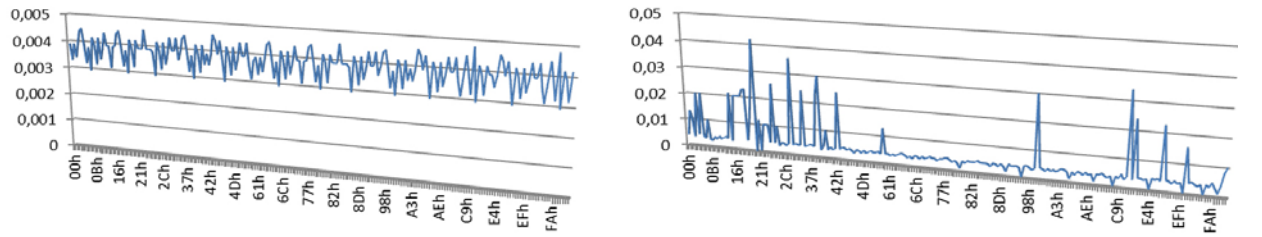
Рассмотрены вопросы построения транслитерационного обратимого кодека для безопасной передачи информации по каналам связи общего пользования. Предложен алгоритм транслитерации, реализуемый с использованием современных информационных технологий и не позволяющий осуществить раскрытие алгоритма и самой передаваемой информации.

Д. Б. Николаев, В. Г. Грибунин[1], С. Н. Колтаков[2], А. А. Скоробогатый[2], А. П. Мартынов

Глобализация информационного пространства, появление большого количества компаний, обеспечивающих различные виды связи, обусловили возможность создания резервных каналов передачи данных по линиям связи общего пользования. При этом необходимо обеспечивать безопасность и целостность передаваемой информации, что зачастую невозможно осуществить средствами, предоставляемыми компаниями-операторами.

В общем виде задача гарантированного обеспечения безопасности при передаче информации сводится к стойкому преобразованию, при этом в качестве преобразователя может выступать как классическая симметричная функция сокрытия, так и асимметричная функция. Результатом преобразования является псевдослучайная информационная структура с заданными характеристиками, базовой из которых является равномерность распределения информации внутри сообщения (кадра, фрейма). На рис. 1 представлены частотные характеристики исходного и преобразованного сообщений. Из рисунка видно, что преобразованные сообщения будут выделяться из всего информационного потока непреобразованных сообщений своей специфической структурой. Данный аспект снижает безопасность передачи преобразованных сообщений по линиям связи общего пользования из-за возможности применения простого вида фильтрации, основанного на частотных закономерностях алфавита сообщения. Кроме этого, современные средства обработки информации позволяют проводить анализ сообщения с использованием встроенных синтаксических и семантических словарей, что не позволяет заменять преобразованные сообщения со специфической структурой несмысловыми выражениями алфавита исходного текста, так как они могут быть отфильтрованы на этапе инкапсуляции в транспортные протоколы.

[1] МОУ «Институт инженерной физики», г. Серпухов.
[2] Генеральный штаб МО РФ.



а б

Рис. 1. Частотные характеристики исходного (а) и преобразованного (б) сообщений

Задачей проводимого исследования является создание транслитерационного обратимого кодека для безопасной передачи информации по каналам связи общего пользования. Общая схема применения «скрывающего» преобразования представлена на рис. 2.

Рис. 2. Схема применения «скрывающего» преобразования

На вход схемы подаются структурированные команды или управляющие последовательности заданного вида, структуру и смысловую нагрузку которых необходимо «скрыть» от «посторонних глаз». Эта входная информация обрабатывается преобразователем исходного текста [1], в качестве которого может использоваться реализация любого криптографического алгоритма (ГОСТ 28147-89, AES и т. д.) или алгоритма, формирующего псевдослучайные последовательности (RC-4, Dragon-128, HC-256 и др.). В результате преобразований данные будут представлены в виде последовательностей с характеристиками, близкими к равномерному распределению (псевдотекст). Как уже было сказано выше, данный тип информации совершенно не стоек к фильтрации, так как имеет отличную от других передаваемых сообщений структуру. Для устранения этого недостатка псевдотекст анализируется и преобразуется в блоке транслитерационного анализа (БТА) с использованием адаптивного полиалфавитного словаря (АПС). После этого полученное сообщение может быть передано в устройства формирования пакетов или другие транспортные системы для передачи, так как воздействие фильтрацией уже не приведет к желаемому результату [2]. На приемном конце полученное смысловое выражение претерпевает обратные преобразования при помощи блока транслитерационной декомпозиции (БТД), использующего АПС, аналогичный словарю для кодирования. Полученный псевдотекст восстанавливается соответствующими криптографическими методами в исходную структурированную команду или управляющую последовательность.

Рассмотрим работу транслитерационного обратимого кодека более подробно. Исходный псевдотекст представляет собой набор случайных символов и может быть представлен в виде последовательности шестнадцатеричных значений длиной l. Ее можно разбить на k блоков фикси-

рованной длины *d*, каждый из которых трансформируется при преобразовании в отдельную единицу (слово) смыслового выражения. В случае некратности псевдотекста принятым для кодирования размерам недостающий блок может быть дополнен нулевыми значениями (рис. 3).

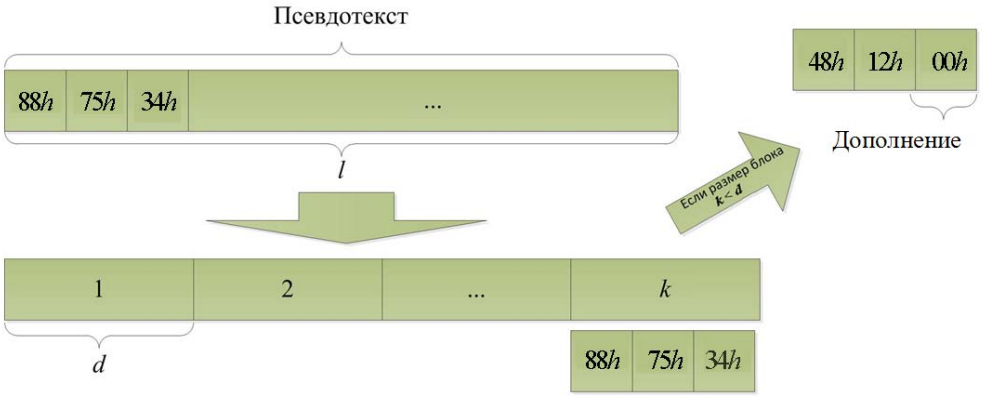


Рис. 3. Процедура подготовки сообщения (формирование блоков заданного размера) к транслитерационному преобразованию

Кодирование конкретного блока осуществляется с использованием АПС. Блок разбивается на две равные части, к каждой из которых добавляется поле контрольной информации (номер слова как функция от длины сообщения). Первая часть блока является номером строки, а вторая – номером столбца матрицы транслитерации, составляющей основу АПС. Ячейка с данными координатами содержит первое слово из смыслового выражения (рис. 4). Далее формируется множество разрешенных комбинаций, логически сочетающихся с первым словом сообщения.

Для оптимизации процедуры поиска приемлемых решений могут использоваться схемы динамического поиска структурированных информационных блоков. В нашем случае в структуре АПС с каждой ячейкой матрицы транслитерации связана лингвоформирующая комбинация (ЛФК), однозначно определяющая множество разрешенных комбинаций. После этого процесс кодирования повторяется для второго блока псевдотекста с той лишь разницей, что в случае непопадания координат блока в разрешенное множество происходит последовательное изменение сначала координаты столбца, а в случае неудачи – координаты строки до попадания в нужную ячейку. При этом для четных блоков происходит увеличение координаты на одну позицию, а для нечетных блоков – уменьшение (рис. 5).

По окончании кодирования второго блока формируется множество разрешенных комбинаций, логически сочетающихся с выражением, состоящим из первого и второго слов сообщения. И процесс кодирования третьего блока осуществляется по вышеописанному сценарию. В результате преобразования всех блоков сообщения формируется логическое лингвистически и синтаксически правильное сообщение, реализующее случайный псевдотекст. Мнемосхема с примером, иллюстрирующим работу транслитерационного обратимого кодека, показана на рис. 6.

Восстановление информации происходит в обратном порядке с использованием ЛФК, упрощающих поиск слова в матрице транслитерации. Корректирующий сдвиг однозначно вычисляется с помощью поля контрольной информации (ПКИ) по номеру блока.

Для расширения функциональности возможно использование внешних семантических корректоров с целью проверки согласования словосочетаний. Такие анализаторы выявляют подозрительные семантические конструкции в тексте и сообщают об этом, тем самым гарантируя отсут-

ствие в тексте определенных классов содержательных ошибок, выявление которых традиционными методами – весьма трудоемкий процесс. Перечень свойств, выявляемых корректором, включает правильность цепочек от задания до использования, а также инварианты, представляющие собой множество равенств термов, истинных в любом состоянии [3]. В этом случае в матрице транслитерации все слова могут располагаться в именительном падеже, что значительно увеличивает пространство возможных комбинаций и повышает безопасность разработанного способа транслитерационного кодирования.

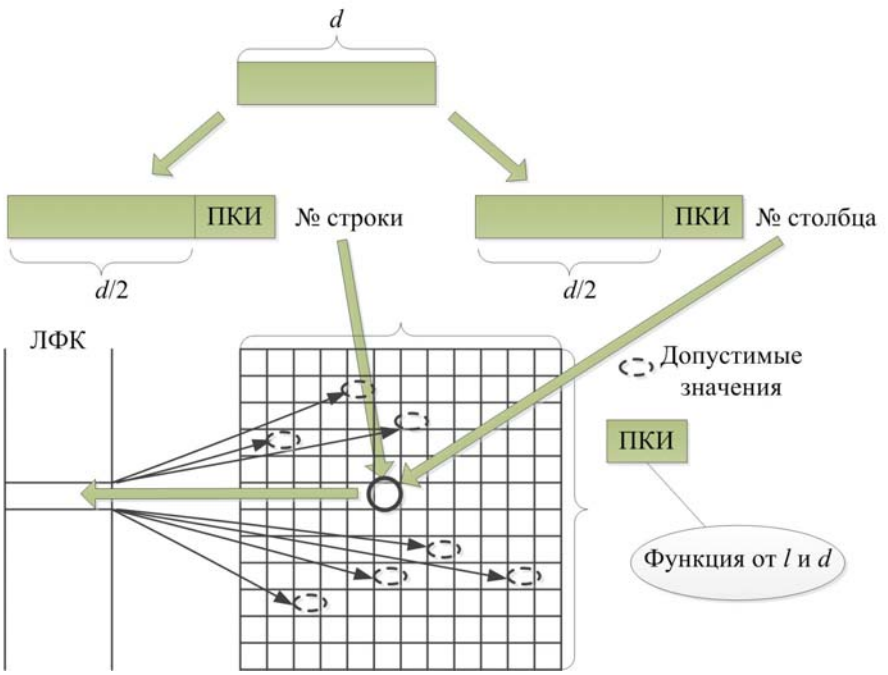


Рис. 4. Процесс формирования логически связанного смыслового выражения

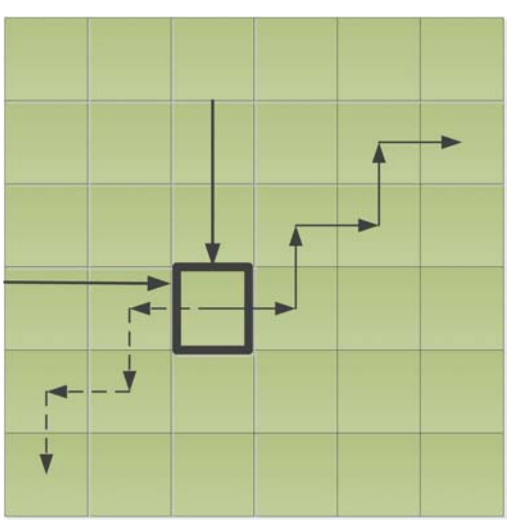


Рис. 5. Процедура поиска слова из разрешенного множества допустимых значений

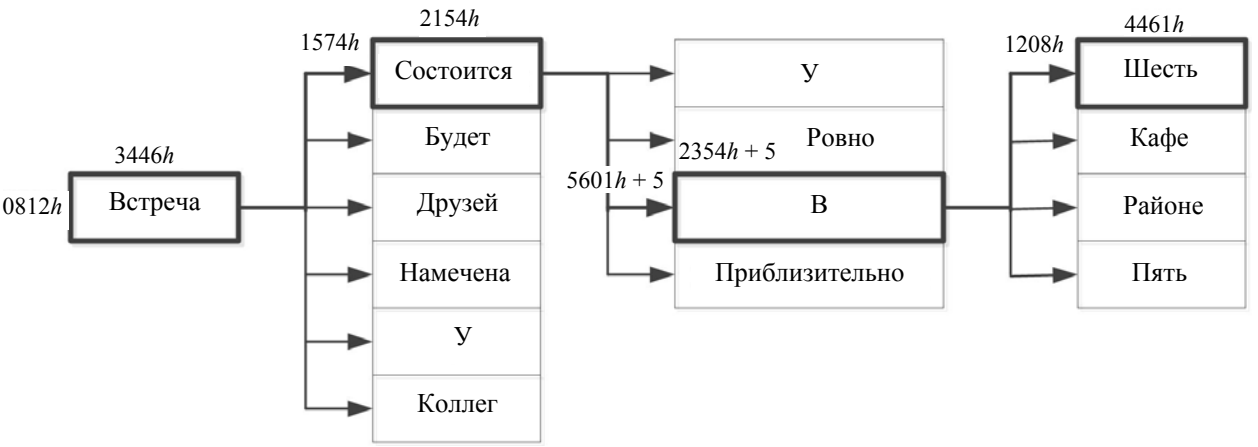


Рис. 6. Мнемосхема, иллюстрирующая работу транслитерационного обратимого кодека

Разработанный транслитерационный обратимый кодек является универсальным и может быть использован для решения ряда аналогичных задач, связанных с обеспечением безопасности информации и повышением удобства использования систем разграничения доступа. Например, условия применения практически всех систем паролирования для дистанционного доступа требуют запоминания достаточно длинного несмыслового пароля, представляющего собой набор разных сочетаний символов, в наилучшем случае, максимально использующем все символы ASCII-кода (0-255 значений (00*h*-*FFh*)). Предложенный кодек позволяет запоминать пароль в виде смысловой фразы, которая автоматически преобразуется в несмысловое случайное сообщение, символы которого выбраны из полностью используемого пространства ASCII-кодов, и циркулирует в системе уже в виде псевдотекста (рис. 7).

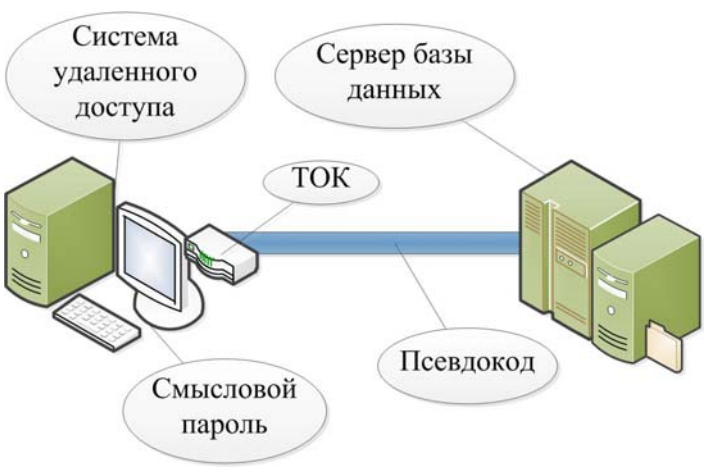


Рис. 7. Применение транслитерационного обратимого кодека в системах паролирования для дистанционного доступа к распределенным базам данных

Список литературы

1. Грибунин В. Г., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред. А. И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011.

2. Кузьмин И. В., Кедрус В. А. Основы теории информации и кодирования: 2-е издание, перераб. и доп. К.: Вища шк., 1986.

3. Поттосин И. В. Российские исследования по языкам программирования и трансляции // МИР ПК – ДИСК, 2003, № 12. Студия программирования, стр. 1/16-16/16.

Working Out of the Transliteration Reversible Codec for Reliable Information Transfer Over Communication Channels of the General Using

D. B. Nikolaev, V. G. Gribunin, S. N. Koltakov, A. A. Skorobogatyj, A. P. Martynov

Questions of convertible codec construction for reliable transfer of the information on general purpose liaison channels are considered. The algorithm of a transliteration effectively enough sold with use of modern information technologies and not allowing to carry out disclosing of algorithm and the most transmitted information is offered.