14. *Knut Donal'd E.* Iskusstvo programmirovaniya [The art of computer programming]. Vol. 4. Issue 3 Generatsiya vsekh sochetaniy i razbieniy [Generating all combinations and partitions]: Translation from English. Moscow: OOO «I.D. Vil'yams», 2007, 208 p.
15. *Grekhem R., Knut D., Patashnik O.* Konkretnaya matematika. Osnovanie informatiki [Concrete mathematics. The Foundation of information science]: Translation from English. Moscow: Mir, 1998, 703 p.
16. *Makov S.V., Shrayfel' I.S.* Otsenka effektivnosti fil'tratsii trafika v mezhsetevykh mostakh i kommutatorakh [Assessment of the effectiveness of traffic filtering in firewall bridges and switches], *Servis v Rossii i za rubezhom* [Services in Russia and abroad], 2011, Vol. 24, No. 5.
17. *Makov S.V., Lityuk V.I.* Organizatsiya tablits fil'tratsii «bez khraneniya adresov» v mezhsetevykh mostakh i kommutatorakh metodom parallel'nogo kheshirovaniya [The organization of tables of the filter "without the" in firewall bridges and switches the parallel method of hashing], *Servis v Rossii i za rubezhom* [Services in Russia and abroad], 2011, Vol. 24, No. 5.
18. *Makov S. et al.* Method of frame filtering table design without searching keys storing, *Proc. IEEE ICSP*, 2014, pp. 1542-1545. ISBN: 978-1-4799-2188-1.
19. *Makov S. V. et al.* A method for ultra fast search-ing within traffic filtering tables in networking hardware, IS&T/SPIE Electronic Imaging. – International Society for Optics and Photonics, 201, pp. 94100M-94100M-7.
20. Cyclone II: Device Handbook. Vol. 1, ALTERA. Available at: http://www.altera.com/ literature/hb/cyc2/cyc2_cii5v1.pdf.

Статью рекомендовал к опубликованию д.т.н., профессор Д.А. Безуглов.

Маков Сергей Владимирович – Донской государственный технический университет; e-mail: makovs@rambler.ru; г. Шахты, ул. Шевченко, 147; тел.: 89281111295; кафедра радиоэлектронных и электротехнических систем и комплексов; к.т.н.; доцент.

Чернышов Дмитрий Юрьевич – e-mail: dimcher@inbox.ru; тел.: 89185767438; кафедра радиоэлектронных и электротехнических систем и комплексов; аспирант.

Тимофеев Дмитрий Витальевич – Южный федеральный университет; e-mail: timofeev.dimitriy@gmail.com; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 89518436972; кафедра теоретических основ радиотехники; аспирант.

Makov Sergei Vladimirovich – Don State Technical University; e-mail: makovs@rambler.ru; 147, Shevchenko street, Shakhty, Russia; phone: +79281111295; the department of radioelectronic and electrotechnique systems and complexes; cand. of eng. sc.; associate professor.

Chernyshov Dmitriy Yurievich – e-mail: dimcher@inbox.ru; phone: +79185767438; the department of radioelectronic and electrotechnique systems and complexes; postgraduate student.

Timofeev Dmitriy Vitalievich – South Federal University; e-mail: timofeev.dimitriy@gmail.com; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: +79518436972; the department of fundamental of radio engineering; postgraduate student.

УДК 004.056.055

К.О. Бондаренко, В.А. Козлов

УНИВЕРСАЛЬНЫЙ БЫСТРОДЕЙСТВУЮЩИЙ АЛГОРИТМ ПРОЦЕДУР ОБЕЗЛИЧИВАНИЯ ДАННЫХ

Целью исследования является разработка модели защиты персональных данных с использованием методов обезличивания данных, обрабатываемых операторами медицинских учреждений. Задачи исследования: исследование существующих методов защиты персональных данных, информационные системы обработки персональных данных организаций здравоохранения с целью выявления актуальных угроз для защиты персональных данных; проведение классификации медицинских информационных систем на типы с точки зрения

защиты персональных медицинских данных; создание модели защиты персональных данных объектов здравоохранения, используя методы обезличивания персональных данных. Представлен универсальный быстродействующий алгоритм обезличивания данных, ориентированный на работу с большими и очень большими массивами. Алгоритм, с целью повышения его быстродействия и упрощения процедур обезличивания данных, ориентирован на работу с сегментированной, реляционной базой данных. Сегментирование базы данных осуществляется путем разбиения ее основных массивов на блоки размерностью по 256 строк в каждом блоке. В состав алгоритмического комплекса включены криптографические примитивы, базирующиеся на трех основных принципах: рассеивания, перемешивания и гаммирования. Криптографическая стойкость системы обеспечивается использованием быстродействующих нелинейных π-алгоритмов, входящих в состав алгоритмов рассеивания и перемешивания. В результате предложен универсальный быстродействующий алгоритм реализации криптографических процедур обезличивания данных ориентированный на работу с большими массивами информации.

Криптографическая защита персональных данных; обезличивание персональных данных; быстродействующие нелинейные алгоритмы перемешивания и рассеивания.

K.O. Bondarenko, V.A. Kozlov

UNIVERSAL QUICK-ACTING ALGORITHM OF THE PROCEDURES OF DATA DEPERSONALIZATION

The goal of the research is to develop a model of personal data protection with use of methods of data depersonalization which are processed by the operators of health care institutions. The tasks of the research: To study the existing methods of personal data protection, information systems of personal data processing in health care institutions in order to identify the actual threats for the personal data protection; to classify medical information systems into the types from the point of view of personal medical data protection; to create a model of protection of personal data of health care institution using methods of data depersonalization. The paper presents universal quick-acting algorithm for data depersonalization. This algorithm is focused on work with large and very large volumes of information as well as on work with a segmented, relational database. Segmenting of the database is done by dividing its main volumes into blocks of 256 lines. The structure of the algorithmic complex includes cryptographic primitives based on three main principles: dispersion, mixing and gammirovanie. Cryptographic resistance of the system is provided by use of quick-acting nonlinear π-algorithms which are the parts of dispersion and mixing algorithms. As a result the paper suggests a universal quick-acting algorithm that provides implementation of cryptographic procedures of data depersonalization. This algorithm is focused on work with large volumes of information.

Cryptographic protection of personal data; personal data depersonalization; quick-acting non-linear algorithms of mixing and dispersion.

Введение. В настоящее время ни одно предприятие не обходится без автоматизированных средств обработки информации. В каждой организации есть информация, которая не должна быть доступна посторонним, а именно – коммерческая тайна, персональные данные, государственная тайна банковская тайна, и т.д. Данные сведении подлежат защите в соответствии с действующим законодательством Российской Федерации, российскими и международными стандартами, регулирующими работу защиты информации, используя при этом программно-аппаратные или технические средства защиты [5–7].

В связи с принятием Государственной думой 08.07.2006 г. Федерального закона № 152-ФЗ, зарегистрированного 27.07.2006 г. «О персональных данных» (с учетом внесенных в него изменений и дополнений от 01.09.2015 г.), и принятием на его основании других нормативно-правовых актовпо обеспечению защиты

информации и персональных данных (ПДн) граждан, обрабатываемых в информационных системах ПДн (ИСПДн), защита ПДн стала актуальной задачей для многих организаций, использующих ПДн граждан, в том числе и медицинских учреждений [1–3].

Постановка задачи. Основным аспектом исследований в области информационной безопасности является разработка новых и совершенствование уже имеющихся методов и средств защиты информации.

Так, например, требования законодательства в области защиты ПДн обязывают все учреждения системы здравоохранения провести ряд организационных и технических мероприятий по их защите [2]. Обеспечение безопасности персональных медицинских данных для учреждений системы здравоохранения является сложной, трудоемкой, затратной работой, ненадлежащее исполнение которой может обернуться значительными негативными последствиями для них и граждан, чьи сведения обрабатываются [5, 6, 10, 16, 17]. При этом всю ответственность за разглашение или утечку несет учреждение, которое занимается вопросами обработки персональных данных.

В связи с этим была поставлена цель – разработка модели защиты персональных данных с использованием методов обезличивания данных, обрабатываемых операторами медицинских учреждений.

При этом объектом исследования выбраны методы защиты персональных данных, обрабатываемые и хранящиеся в медицинских информационных системах лечебно-профилактических учреждений.

Результатом исследований в рассматриваемой статье является универсальный быстродействующий алгоритм процедур обезличивания данных.

1. Основные аспекты обезличивания данных. В соответствии со ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных [1, 4].

Хранение персональных данных в обезличенном виде, как известно [3, 8, 14], способствует заметному снижению уровня таких требований, что в свою очередь приводит к существенному сокращению издержек, связанных с их хранением и обработкой.

В результате обезличивания данных разрывается связь свободно хранимых в массивах базы данных отдельных реквизитов с конкретными субъектами, которым они принадлежат. Другими словами, совокупность персональных данных, принадлежащих отдельному субъекту, разбивается на отдельные реквизиты, которые «отрываются» от субъекта путем перемешивания в рамках базы по определенному алгоритму.

Для восстановления связей субъекта с его реквизитами администратору должна быть известна некая секретная комбинация (пароль, ключ), которую он должен держать в строгом секрете. Однако затраты на ее хранение несоизмеримо меньше, чем засекречивание всей базы, так как объем засекреченной информации сокращается в десятки тысяч раз (с увеличением размерности самой базы резко возрастает и величина этого соотношения).

В работе [15] описаны процедура и алгоритм обезличивания персональных данных, которые успешно решают эту задачу. Однако при больших размерах объема информации в базе данных работа алгоритма будет недостаточно эффективной, так как в его основе лежат алгоритмы поиска информации по коду (идентификатору) строки в массивах базы данных. А это, как известно, при больших размерах массивов существенно замедляет быстродействие поиска.

С целью повышения быстродействия алгоритмов поиска крупные массивы разбивают на целый ряд подмассивов, в рамках которых и реализовано перемешивание как основное средство обезличивания. Но такая процедура, во-первых, снижает уровень секретности (в перемешивании участвуют только те реквизиты, которые попали в данный конкретный подмассив, при этом некоторые из них могут случайно совпадать), и, во-вторых, такой подход весьма неэффективен в случае выборочных запросов на группу субъектов, которые с большой степенью вероятности могут находиться в разных подмассивах, со всеми вытекающими отсюда последствиями.

Предлагаемый авторами вариант решения этой задачи ориентирован, во-первых, на алгоритмы с поиском информации в таблицах не по коду, а по номеру строки, и, во-вторых, сама процедура перемешивания заменена более эффективной с точки зрения ее быстродействия, так называемой процедурой квазиперемешивания – алгоритмом, который любой реквизит заменяет на любой другой, принадлежащий данному множеству реквизитов.

2. Разработка универсального быстродействующего алгоритма процедуры обезличивания данных. Как известно, практическая реализация большинства процедур, связанных с перемешиванием данных в массивах и справочниках большой размерности, приводит к необходимости рационального подхода к алгоритмам поиска информации с точки зрения их универсальности и быстродействия.

Поэтому вторым не менее важным аспектом является применение исключительно реляционных баз данных, работающих с табличными массивами и справочниками, столбцы и строки которых строго фиксированной длины, что позволяет в десятки раз повысить скорость их обработки.

В данном случае адрес любой ячейки справочника или массива ($A_{n,m}$) легко и быстро определяется элементарной расчетной формулой:

$$A_{n,m} = B_t + (n-1)\cdot D_n + \sum_{i=1}^{i=m-1} D_i \ , \qquad (1)$$

B_t – базовый адрес таблицы;

n, m – номер строкии номер столбца;

m – номер столбца;

D_n, D_m – длина строки идлина столбца соответственно.

Инициализация базы данных. Итоговая таблица индивидуальных данных (T1.Itog), требующих обязательного обезличивания по каждому пользователю имеет следующий вид.

Таблица T1. Itog

Идентификатор пользователя (P_i)	Атрибуты					
	Атрибут A_{1i}	Атрибут A_{2i}	Атрибут A_{3i}	Атрибут A_{4i}	…	Атрибут A_{mi}
P_1	A_{11}	A_{21}	A_{31}	A_{41}	…	A_{m1}
P_2	A_{12}	A_{22}	A_{32}	A_{42}	…	A_{m2}
…	…	…	…	…	…	…
P_n	A_{1n}	A_{2n}	A_{3n}	A_{4n}	…	A_{mn}

Таблица T1.Itog, как и все другие таблицы, входящие в состав базы данных, формируются по правилам реляционных таблиц, строки которых будем называть записями, а столбцы – полями этих логических записей. Операции выборки, вставки, обновления и удаления выполняются с помощью специальных операторов на языке баз данных SQL [9], который является официальным стандартом языка, ори-

ентированного на обработку реляционных систем. Идентификаторы атрибутов могут быть представленыв единичной или множественной форме. Для раскрытия множественной формы, когда для конкретного пользователя имеется сразу несколько единиц данного атрибута, формируются специальные таблицы множественных форм по каждому атрибуту.

Кроме того, формируется еще одна таблица (T2.Fio), в которой каждому идентификатору $\mathbf{P_i}$ ставятся в соответствие личные данные пользователя, которые нет необходимости обезличивать.

Таблица T2. Fio

Идентификатор пользователя (P_i)	Атрибуты					
	Фамилия	Имя	Отчество	Год рождения	…	Адрес прописки
P_1	F_1	I_1	O_1	Y_1	…	A_1
P_2	F_2	I_2	O_2	Y_2	…	A_2
…	…	…	…	…	…	…
P_n	F_n	I_n	O_n	Y_n	…	A_n

Помимо описанных выше базовых таблиц, формируется базовое множество таблиц идентификации атрибутов. Каждая такая таблица (T3.Ai) содержит полный перечень возможных значений реквизитов по данному конкретному атрибуту.

Таблица T3. Ai

Идентификатор атрибута (A_i)	Значение атрибута
A_{1i}	Значение атрибута A_{1i}
A_{2i}	Значение атрибута A_{2i}
…	…
A_{N_i}	Значение атрибута A_{N_i}

На стадии инициализации базы данных в среде SQL осуществляется идентификация связей таблиц T1 и T2 с таблицами из множества T3, в процессе которой все идентификаторы заменяются их фактическими адресами (так называемыми вторичными идентификаторами), что и предопределяет высокую скорость их взаимодействия.

Обезличивание данных. С целью повышения быстродействия и упрощения процедур обезличивания данных таблица T1.Itog разбивается на ряд сегментов по 256 строк в каждом. Последний сегмент, при необходимости, дополняется недостающим количеством строк, заполненных символами-заполнителями. Далее все операции по обезличиванию данных выполняются последовательно по каждому сегменту в отдельности.

Такое число строк в каждом сегменте выбрано неслучайно, так как в криптографии в процессе обработки электронных документов в качестве алфавита принято использовать всю таблицу ASCII-символов, т.е. множество всевозможных целых неотрицательных чисел от 0 до 255 с определенными на нем операциями сложения и вычитания по модулю 256. Такую конструкцию в математике еще называют кольцом вычетов по модулю 256 и обозначают как Z/256.

Алгоритмы симметричного шифрования базируются на применении в различных сочетаниях всего трех принципов: рассеивания, перемешивания и гаммирования.

Рассеивание представляет собой распространение влияния каждого символа открытого текста на каждый символ шифртекста, что позволяет скрыть статистические свойства открытого текста.

Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств.

Гаммирование по своей сути представляет механизм, позволяющий «растянуть» секретный ключ (секретную ключевую комбинацию) до размеров шифруемого сообщения, с целью как можно большего приближения алгоритмов криптографических преобразований к уровню криптографической стойкости шифровального блокнота, т.е. к уровню абсолютной криптостойкости. В симметричных системах, и в частности в алгоритмах гаммирования, очень часто используется маркант (Merchant) или вектор инициализации, который имеет небольшую размерность и присутствует в незашифрованном виде в головном сегменте таблицы T1.Itog [11, 12].

Маркант позволяет при шифровании одним и тем же ключом одного и того же исходного текста получать отличные друг от друга результаты шифрации. Хранить его в тайне не обязательно, при этом он должен быть случайным и непредсказуемым. Применение марканта сочетается с использованием генератора псевдослучайных чисел (ГПСЧ) совместно с алгоритмом гаммирования, что позволяет, используя в качестве начальных условий для ГПСЧ секретного ключа и марканта, «растянуть» гамму до размера шифруемого сегмента (в нашем случае до 256 байт).

Для реализации процедур обезличивания данных будем использовать последние два принципа (перемешивания и гаммирования), так как принцип рассеивания предполагает реализацию процедур подстановки, т.е. замены в нашем электронном документе одних символов на другие. Однако нас такого рода операции не устраивают, так как после их реализации усложняются процедуры статистического анализа содержимого основной таблицы T1.Itog.

Процедуры перемешивания будем применять к каждому сегменту таблицы T1.Itog в отдельности. Перемешивание внутри сегмента будем производить двух типов: *построчное*, т.е. менять местами строки, «отрывая» их от идентификатора строки, и *атрибутное* – меняя местами значения атрибутов в рамках отдельного столбца данного сегмента.

В основу алгоритма обезличивания данных положим совокупность нелинейных комбинированных π-алгоритмов, входящих в состав системы симметричных криптографических преобразований и отличающихся высоким быстродействием и высокой криптостойкостью [13, 18–20].

На первом этапе формируются специальные рабочие массивы R_i. Для их создания формируется одномерный массив (M_1) однобайтных элементов из 256 строк, со значениями от 0 до 255. Перемешав его элементы, получаем рабочие массивы – R_i, с помощью которых реализованы нелинейные π-алгоритмы построчного и атрибутного перемешивания.

Таким образом, все массивы R_i типа char размерностью 256 байт каждый – это массивы, в которых некоторым образом перемешаны все возможные значения из множества типа char. Нуль может быть в нем на *35* месте, *1* – на *147* и так далее. Но в нем обязательно должны быть и *0*, и *1*, и вся остальная таблица *ASCII*-символов.

Такого рода процедура перемешивания называется прямой подстановкой и обозначается как $\boldsymbol{\pi}$. А обратная подстановка – это когда в этой таблице адреса и значения меняются ролями: что было адресом становится значением, а значение – адресом. И обозначается обратная подстановка как $\boldsymbol{\pi}^{-1}$.

С точки зрения программной реализации такого рода преобразования называются **π**-нелинейными и являются весьма быстродействующими и эффективными с точки зрения их нелинейности.

Модуль создания рабочих массивов R_i. Алгоритм формирования рабочих массивов R_i состоит из 128 циклов. В каждом цикле значения одной пары строк n_j и n_k меняются местами. Номера строк n_j и n_k представляют собой соответствующие элементы гамма-последовательности, которые вырабатываются криптостойким ГПСЧ (генератором псевдослучайных чисел).

В качестве надежного ГПСЧ можно использовать любой криптостойкий блочный шифр в режиме получения хэш-функции. При этом в качестве первого блока необходимо использовать маркант и секретный ключ. В этом случае генерируемая последовательность будет состоять из набора зашифрованных блоков. Для дешифрации любого блока этой последовательности необходимо знать секретный ключ шифрования. Таким образом, задача вскрытия гамма-последовательности сводится к взлому блочного шифра.

Алгоритм разбиения исходника (табл.T1.Itog) на сегменты. Нашей отправной точкой является тот факт, что мы должны ориентироваться на работу с большими и очень большими массивами информации, именно в такой ситуации и проявляется главное преимущество симметричных алгоритмов криптографических преобразований – их быстродействие (в нашем случае это табл. T1.Itog с атрибутами, требующими обязательного обезличивания). Поэтому разработка алгоритма перемешивания, охватывающего всю табл. T1.Itog одновременно, – это, конечно же, очень «круто», но весьма не рационально, так как приведет к существенным потерям в быстродействии системы в целом при невысокой ее криптостойкости.

Куда более целесообразным представляется разбить нашу таблицу на небольшие, одинаковой размерности сегменты, дополнив самый последний сегмент до стандартной размерности символами-заполнителями. Самым оптимальным вариантом размерности такого сегмента, с точки зрения быстродействия и простоты обработки, будут сегменты размерностью 256 строк каждый. Таким образом, на предварительном этапе разбиваем табл. T1.Itog на сегменты по 256 строк каждый. Последний сегмент при необходимости дополняем до 256 строк символами-заполнителями.

Алгоритм пошагового построчного перемешивания табл. T1.Itog в рамках отдельного сегмента. Алгоритм является многовариантным и оформлен в виде модуля π-нелинейного двухэтапного внутрисегментного перемешивания. Каждый вариант алгоритма обеспечивает обработку одного 256-строкового сегмента табл. T1.Itog.

Выбираем из множества R_i два одномерных рабочих массива (например, R_1 и R_2) по 256 однобайтных строк в каждом. Каждая строка содержит уникальное значение отличное от остальных, в пределах от 0 до 255. Значения строк этих двух массивов не совпадают и определяются по специальному алгоритму, описанному выше. Затем выбираем соответствующий 256-строковый сегмент табл. T1.Itog.

Схема сопряжения выбранного сегмента с рабочими массивами R_1 и R_2 по предлагаемому алгоритму показана на рис. 1. Первая колонка каждого массива содержит порядковые номера строк, значения которых в памяти не прописаны, а изображены исключительно для наглядности.

Алгоритм перемешивания состоит из двух этапов: на первом этапе перемешивание осуществляется с использованием рабочего массива R_1, на втором – R_2. Рассмотрим более подробно первый этап работы алгоритма:

- определяем значение первой строки рабочего массива R_1: в нашем случае $R_{1,1}$ = 12 (см. рис. 1, для наглядности размерность массива не 256, а 16 строк);
- обращаемся к строке $R_{1,1}$ исходника (к 12 строке массива S) и считываем значение в строке S_{12};
- найденное значение из таблицы переписываем в первую строку массива Z_1;
- переходим к обработке следующей строки массива R_1 и т.д.

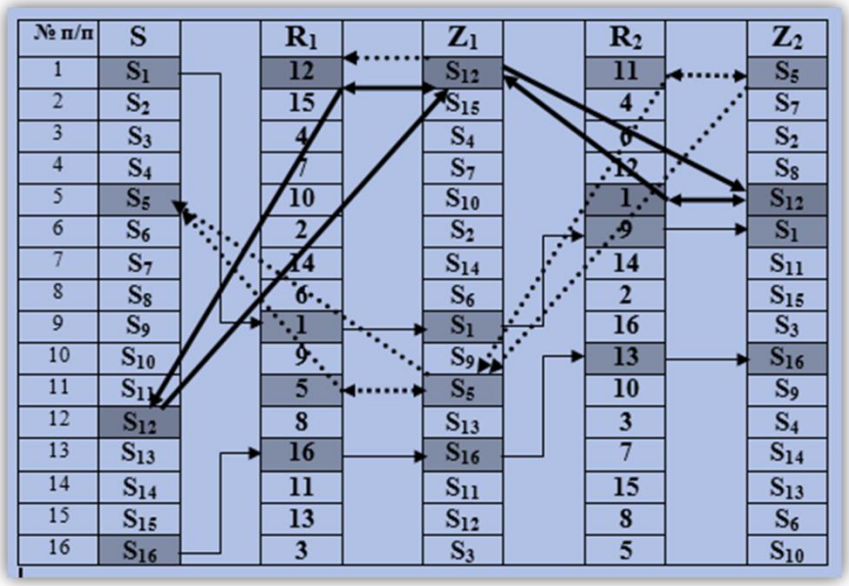

Рис. 1. Схема последовательности перемещения элементов из массива S в массив Z_1 и далее из массива Z_1 в массив Z_2

В результате получаем полностью перемешанный блок исходного текста размерностью 256 байт. Обозначим его Z_1. На втором этапе используем тот же алгоритм с новыми параметрами: Z_1 – вместо S, R_2 – вместо R_1 и Z_2 – вместо Z_1. Двухэтапный алгоритм перемешивания не содержит в своем составе операций поиска строки по ее коду (имеются лишь обращения по номеру строки), что переводит его в разряд супербыстродействующих, а его двухэтапность говорит о том, что он обладает вторым порядком π-нелинейности с высокой степенью криптостойкости.

Обратная процедура, т.е. процедура дешифрации, заключается в следующем: из первой строки массива R_2 считываем значение (в нашем случае $R_{2,1}$ = 11, как показано на рис. 1); обращаемся к первой строке исходника – массива Z_2 (в нашем примере $Z_{2,1} = S_5$); записываем значение первой строки массива Z_2 (S_5) в 11 строку массива Z_1; переходим к обработке следующей строки рабочего массива R_2 и т.д. Для наглядности на этом же рисунке представлена схема перемещений элементов (S_1 и S_{16}) для алгоритма, ориентированного на поиск элементов по их значениям в рабочих массивах R_1 и R_2. Так, для элемента S_1 схема перемещений выглядит следующим образом: S_1→поиск в массиве R_1 строки со значением $R_{1,x}$ = 1 (9 строка) →запись в 9 строку массива Z_1 значения S_1→поиск в массиве R_2 строки со значением $R_{2,x}$ = 9 (6 строка) и т.д. Максимально возможное количество

вариантов алгоритма зависит от числа рабочих массивов, входящих в состав множества $\{R_i\}$, и определяется по формуле **N = n (n-1)**, где N – возможное количество вариантов алгоритма, а n – количество рабочих массивов множества $\{R_i\}$.

Алгоритм пошагового перемешивания реквизитов j-го столбца отдельного сегмента табл. T1.Itog. После перемешивания строк сегмента необходимо перемешать реквизиты в каждом отдельном столбце, содержащем информацию, подлежащую обезличиванию. Алгоритм перемешивания реквизитов столбца также является многовариантным, он перемешивает не строки сегмента, а только реквизиты его отдельного столбца.

Вариант первый – на каждом шаге меняются местами j-я и k-я ячейки данного столбца сегмента. Номера перемешиваемых на первом шаге ячеек прописаны соответственно в 1-й и 2-й строках одного из рабочих массивов R_i, на втором шаге – в 3-й и 4-й строках и т.д. Всего таких итераций 128.

Вариант второй отличается от первого лишь тем, что номера перемешиваемых ячеек извлекаются на первом шаге теперь из 1-й и 3-й строк рабочего массива R_i, на втором шаге – из 2-й и 4-й строк и т.д.

Другой возможной серией вариантов алгоритма является извлечение номеров перемешиваемых ячеек не из одного, а из двух разных массивов R_i. Например, для 1-го шага из 1-ой строки рабочего массива R_1 и из 2-й строки рабочего массива R_2.

Процесс дешифрации работает от обратного – меняет (для первого варианта алгоритма) на первом шаге местами ячейки соответствующего столбца табл. T1.Itog, номера которых прописаны в 256 и 255 строках массива R_i. Алгоритм не использует процедуры поиска в массивах, относится к классу **π**-нелинейных первого порядка, обладает высоким быстродействием и криптостойкостью. Почему процедура перемешивания не распространяется на межстолбцовое перемешивание обезличиваемых реквизитов сегмента? Дело заключается в том, что в случае межстолбцового перемешивания полностью утрачивается возможность какого-либо статистического анализа обезличенных реквизитов по каждому столбцу в отдельности или сегменту в целом, без восстановления их обезличенности.

Модуль элементарной подстановки (процедура квазиперемешивания) для обработки j-го столбца отдельного сегмента табл. T1.Itog.

Процедура квазиперемешивания (реализованная в виде модуля элементарной подстановки) работает только с теми столбцами сегмента, в которых содержится строго конфиденциальная информация. Процедура как бы осуществляет квазиперемешивание идентификаторов атрибутов не внутри сегмента, а в масштабах массива, содержащего полный перечень возможных значений идентификаторов по данному атрибуту. Идентификатором в данном случае является порядковый номер строки соответствующей таблицы идентификаторов атрибутов – T3.Ai.

К каждой ячейке j-го столбца прибавляется значение из ячейки рабочего массива R_2 с тем же порядковым номером ячейки, что и порядковый номер символа исходного текста в данном блоке, при этом операция сложения производится по модулю A_{N_i} .

$$A_i = (A_i + R_{j,i}) \bmod A_{N_i},$$

где i – порядковый номер атрибута в исходном тексте и символа в рабочем массиве R_j; A_i – цифровой код i-го символа исходного текста; R_{ji} – цифровой код i-й ячейки рабочего массива R_j; A_{N_i} – порядковый номер последнего элемента i-го атрибута.

На первый взгляд криптостойкость данного алгоритма подстановки весьма сомнительна. Однако в сочетании с алгоритмом нелинейного π-перемешивания, криптоаналитику без знания первоначального порядкового номера символа в исходном тексте просто не за что «зацепиться».

Выводы. Таким образом, совокупность базовых алгоритмов шифрования баз данных позволяет получить достаточный уровень обезличивания персональных данных при относительно небольшом увеличении затрат процессорного времени и пропускной способности сетевых интерфейсов по сравнению с другими алгоритмами шифрования, не обеспечивающими такой же уровень обезличивания. В перспективе развития данного алгоритма возможно сокращение времени поиска за счет выполнения поиска по защищенному массиву индексации с последующей обработкой лишь необходимых данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» с изменениями и дополнениями от 01.09.2015 г.
2. Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 20.07.2013) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".
3. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996, утвержденные 13.12.2013 г. Руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.
4. Приказ Роскомнадзора от 05.09.2013 No. 996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ") (Зарегистрировано в Минюсте России 10.09.2013 No. 29935).
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России от 15.02.2008 г.
6. Приказа ФСТЭК от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
7. «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. №. 55/86/20.
8. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = AppliedCryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с. – ISBN 5-89392-055-4.
9. *Дейт К.Дж.* Введение в системы баз данных: пер. с англ. – СПб.: Издательский дом «Вильямс», 2003. – 848 с.
10. *Зыков В.Д., Мещеряков Р.В., Беляков К.О.* Защита персональных медицинских данных в автоматизированных медицинских информационных системах лечебно-профилактических учреждений // Безопасность информационных систем: доклады ТУСУРа. – Июнь 2009. – № 1 (19). – Ч. 2. – С. 67-69.
11. *Козлов В.А., Чернышев А.Б. и др.* Вероятностная модель системы асимметричных криптографических преобразований // Научное обозрение. – 2015. – № 5. – С. 261-266.
12. *Козлов В.А., Чернышев А.Б.* Вероятностная модель электронной цифровой подписи // Научное обозрение. – 2015. – № 11. – С. 141-146.
13. *Масленников М.Е.* Практическая криптография. – СПб.: БХВ-Петербург, 2003. – 464 с.
14. *Фергюсон Н., Шнайер Б.* Практическая криптография. – М.: Изд-во «Вильямс», 2005. – 416 с.

15. *Саксонов Е.А., Шередин Р.В.* Процедура обезличивания персональных данных // Наука и образование. Эл №ФС 77-30569, март 2011. – Режим доступа: http://technomag.edu.ru/doc/173146.html.
16. *Minayev1 Yu.L., Lazareva N.V., Illarionova E.V.* Opportunity, safety and prospects of use of medical information systems // The journal of scientific articles “Health & education millennium”. – 2013. – Vol. 15, No. 1-4.
17. *Ya. I.–O. Guliev, Vogt I.A., Vogt O.A., Belyakin A.J.* Healthcare Information System and Information Safety. Problems and solutions // Proceedings of Program Systems institute scientific conference “Program systems: Theory and applications”. – Pereslavl-Zalesskij. – 2009. – Vol. 2. – P. 175-206.
18. CryptDB: HOWTO Compile on Ubuntu Linux 12.04 [Электронный ресурс]. – Режим доступа: http://whitehatty.wordpress.com/2012/09/30 /cryptdb-howto-compile-on-ubuntu-linux-12-04/, свободный.
19. *Floyer D., Kelly J., Vellante D., Miniman S.* Big Data Database Revenue and Market Forecast 2012–2017 // Professional community Wikibon. – Режим доступа: http://wikibon.org/wiki/v/Big_Data_Database_Revenue _and_Market_Forecast_2012–2017, свободный.
20. Magic Quadrant for Data Masking Technology // Gartner. – 2013. – Режим доступа: https://www.gartner.com/doc/2636081, свободный.

REFERENCES

1. Federal'nyy zakon Rossiyskoy Federatsii ot 27 iyulya 2006 g. № 152-FZ «O personal'nykh dannykh» s izmeneniyami i dopolneniyami ot 01.09.2015 g [Federal law of the Russian Federation of 27 July 2006 No. 152-FZ "On personal data" with changes and additions from 01.09.2015].
2. Postanovlenie Pravitel'stva RF ot 21.03.2012 № 211 (red. ot 20.07.2013) "Ob utver-zhdenii perechnya mer, napravlennykh na obespechenie vypolneniya obyazannostey, predusmotrennykh Federal'nym zakonom "O personal'nykh dannykh" i prinyatymi v sootvetst-vii s nim normativnymi pravovymi aktami, operatorami, yavlyayushchimisya gosudarstvennymi ili munitsipal'nymi organami" [The decree of the Government of the Russian Federation dated 21.03.2012 No. 211 (as amended on 20.07.2013) "About the assertion the statement of the list of measures aimed at ensuring compliance with obligations contained in the Federal law "On personal data" and adopted in accordance with the USA in accordance with it normative legal acts, the operators, which is a public-governmental or municipal authorities"].
3. Metodicheskie rekomendatsii po primeneniyu prikaza Roskomnadzora ot 5 sentyabrya 2013 g. № 996, utverzhdennye 13.12.2013 g. Rukovoditelem Federal'noy sluzhby po nadzoru v sfere svyazi, informatsionnykh tekhnologiy i massovykh kommunikatsiy [Methodical recommendations on the application of the order of Roscomnadzor on September 5, 2013 No. 996 approved 13.12.2013. the Head of the Federal service for supervision in the sphere of Telecom, information technologies and mass communications].
4. Prikaz Roskomnadzora ot 05.09.2013 N 996 "Ob utverzhdenii trebovaniy i metodov po obezlichivaniyu personal'nykh dannykh" (vmeste s "Trebovaniyami i metodami po obezlichivaniyu personal'nykh dannykh, obrabatyvaemykh v informatsionnykh sistemakh personal'nykh dannykh, v tom chisle sozdannykh i funktsioniruyushchikh v ramkakh realizatsii federal'nykh tselevykh programm") (Zaregistrirovano v Minyuste Rossii 10.09.2013 N 29935) [The order of Roskomnadzor from 05.09.2013 N 996 "On approving the requirements and methods for the depersonalization of personal data" (together with "the Requirements and methods for the depersonalization of personal data processed in personal data information systems, including established and operating within the framework of implementation of Federal programs") (Registered in Ministry of justice of Russia 10.09.2013 No. 29935)].
5. Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. FSTEK Rossii ot 15.02.2008 g. [The basic model of threats to the security of personal data during processing in personal data information systems. The FSTEC of Russia from 15.02.2008].

6. Prikaza FSTEK ot 18 fevralya 2013 g. № 21 "Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh" [The order of FSTEC of February 18, 2013 No. 21 "On approval of Composition and content of organizational and technical measures for personal data security at their processing within information systems of personal data"].
7. «Poryadkom provedeniya klassifikatsii informatsionnykh sistem personal'nykh dannykh», utverzhdennym prikazom FSTEK Rossii, FSB Rossii i Mininformsvyazi Rossii ot 13 fevralya 2008 g. №. 55/86/20 ["Procedure of classification of personal data information systems" approved by the order of the FSTEC of Russia, FSB of Russia and the Ministry of communications of Russia dated 13 February 2008 No. 55/86/20].
8. *Bryus Shnayer*. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si = AppliedCryptography. Protocols, Algorithms and Source Code in C [Applied cryptography. Protocols, algorithms, and source code in C language = AppliedCryptography. Protocols, Algorithms and Source Code in C]. Moscow: Triumf, 2002, 816 p. ISBN 5-89392-055-4.
9. *Deyt K.Dzh.* Vvedenie v sistemy baz dannykh [Introduction to database systems]: Translation from English. St. Petersburg: Izdatel'skiy dom «Vil'yams», 2003, 848 p.
10. *Zykov V.D., Meshcheryakov R.V., Belyakov K.O.* Zashchita personal'nykh meditsinskikh dannykh v avtomatizirovannykh meditsinskikh informatsionnykh sistemakh lechebno-profilakticheskikh uchrezhdeniy [Protection of personal medical data in automated medical information systems medical-preventive institutions], *Bezopasnost' informatsionnykh sistem: Doklady TUSURa* [the Security of information systems: Reports at Tomsk University], June 2009, No. 1 (19), Part 2, pp. 67-69.
11. *Kozlov V.A., Chernyshev A.B. i dr.* Veroyatnostnaya model' sistemy asimmetrichnykh kriptograficheskikh preobrazovaniy [A probabilistic model of the system asymmetrical creep-map transformations], *Nauchnoe obozrenie* [Scientific Review], 2015, No. 5, pp. 261-266.
12. *Kozlov V.A., Chernyshev A.B.* Veroyatnostnaya model' elektronnoy tsifrovoy podpisi [A probabilistic model of the digital signature], *Nauchnoe obozrenie* [Scientific Review], 2015, No. 11, pp. 141-146.
13. *Maslennikov M.E.* Prakticheskaya kriptografiya [Practical cryptography]. St. Peresburg: BKhV-Peterburg, 2003, 464 p.
14. *Nil's Fergyuson, Bryus Shnayer*. Prakticheskaya kriptografiya [Practical cryptography]. Moscow: Izd-vo Vil'yams, 2005, 416 p.
15. *Saksonov E.A., Sheredin R.V.* Protsedura obezlichivaniya personal'nykh dannykh [The procedure for anonymisation of personal data], *Nauka i obrazovanie* [Science and Education]. El №FS 77-30569, mart 2011. Available at:http://technomag.edu.ru/doc/173146.html.
16. *Minayev1 Yu.L., Lazareva N.V., Illarionova E.V.* Opportunity, safety and prospects of use of medical information systems, *The journal of scientific articles "Health & education millennium"*, 2013, Vol. 15, No. 1-4.
17. *Ya. I.–O. Guliev, Vogt I.A., Vogt O.A., Belyakin A.J.* Healthcare Information System and Information Safety. Problems and solutions, *Proceedings of Program Systems institute scientific conference "Program systems: Theory and applications".* Pereslavl-Zalesskij, 2009, Vol. 2, pp. 175-206.
18. CryptDB: HOWTO Compile on Ubuntu Linux 12.04. Available at: http://whitehatty.wordpress.com/2012/09/30 /cryptdb-howto-compile-on-ubuntu-linux-12-04/.
19. *Floyer D., Kelly J., Vellante D., Miniman S.* Big Data Database Revenue and Market Forecast 2012–2017, *Professional community Wikibon*. Available at: http://wikibon.org/wiki/v/ Big_Data_Database_Revenue _and_Market_Forecast_2012–2017.
20. Magic Quadrant for Data Masking Technology, *Gartner*, 2013. Available at: https://www.gartner.com/doc/2636081.

Статью рекомендовал к опубликованию д.т.н. В.П. Иосифов.

Бондаренко Карине Овиковна – Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске; e-mail: karinamailto@mail.ru; 357538, г. Пятигорск, ул. Ессентукская, 78-1-29; тел.: 89187594749; кафедра информационной безопасности, систем и технологий; старший преподаватель.

Козлов Владимир Александрович – кафедра информационной безопасности, систем и технологий; доцент, к.т.н.

Bondarenko Karine Ovikovna – Institute of services, tourism and Design (Branch) SKFU in Pyatigorsk; e-mail: karinamailto@mail.ru; 78-1-29, Essentukskaya street, Pyatigorsk, 357538, Russia; phone: +79187594749; the department of information security, systems and technologies; senior lecturer.

Kozlov Vladimir Aleksandrovich – the department of information security, systems and technologies; assistant professor, candidate of technical sciences.

УДК 621.39

И.А. Енгибарян, Б.Х. Кульбикаян, О.А. Сафарьян

ИСПОЛЬЗОВАНИЕ СВОЙСТВА СИНЕРГИЧНОСТИ ДЛЯ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ СВЯЗИ

В статье на примере фрагмента системы сотовой связи «центр коммутации-базовые станции» рассматриваются вопросы проявления свойства синергичности в радиотехнических системах, содержащих большое число одновременно и независимо работающих генераторов. Показано, что возможность проявления данного свойства связана с введением дополнительных связей в системе, позволяющих на основе одновременного измерения фаз несущих сигналов, формируемых данными генераторами, получать оценку отклонения частоты генератора от номинального значения с дисперсией меньшей, чем нестабильность любого генератора в данной системе. В качестве показателя синергичности рассматривается помехоустойчивость системы, определяемая как вероятность ошибки при демодуляции одного бита цифрового потока. Приведены результаты исследований, позволяющие оценить проявление свойства синергичности в зависимости от числа генераторов, входящих в систему связи. С использованием численного моделирования получена оценка выигрыша в снижении вероятности битовой ошибки в зависимости от параметров системы, определяющих ее синергичность (числа генераторов и их относительных нестабильностей). В частности, в условиях рассматриваемого примера показано, что проявление свойства синергичности обеспечивает повышение стабильности генераторов в 2…10 раз и повышение помехоустойчивости системы на порядок.

Система связи; помехоустойчивость системы связи; синергичность; стабильность частоты; вероятность битовой ошибки.

I.A. Engibaryan, B.Kh. Kulbikayan, O.A. Safar'yan

USING THE SYNERGY PROPERTIES TO IMPROVE NOISE IMMUNITY OF COMMUNICATION SYSTEMS

On the example of the part of communication system "switching centre-base station" the existence of properties of synergy in electronic systems containing a large number of simultaneously and independently operating generators examines in the article. It is shown that the possibility of the existence of this property is related to the introduction of additional links in the system that allows for simultaneous measurement of the phases of the carrier signals generated by these generators to obtain an estimate of the deviation of the oscillator frequency from the nominal value with a smaller variance than the volatility of any generator in the system. As an indicator of synergy considers the interference immunity of the system, defined as the probability of error in demodulating one-bit digital stream. The results of the researches, allowing to estimate the manifestation of the properties of synergy depending on the number of generators included in the communication system. Using numerical simulation, the evaluation of the gain in reducing the probability of bit error, depending on the system parameters that determine its synergies (number of genera-