Раздел I. Алгоритмы обработки информации

УДК 004.056.55 DOI 10.18522/2311-3103-2020-5-6-16

Л.К. Бабенко, А.С. Шумилин, Д.М. Алексеев

АЛГОРИТМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ХРАНЕНИЯ И ОБРАБОТКИ РЕЗУЛЬТАТОВ ОБСЛЕДОВАНИЙ*

Цели исследования состоят в разработке и оценке эффективности структуры облачной платформы хранения, обработки и систематизации медицинских данных, определении метода защиты, в частности, обеспечения конфиденциальности при передаче и хранении результатов обследований. Для достижения поставленной цели решаются задачи анализа существующих моделей информационных процессов и структур в предметной области, особенности средств накопления и обработки медицинских данных, хранящихся в электронных информационных системах учёта пациентов, разрабатывается архитектура облачной платформы распределенного хранения данных и алгоритм обеспечения безопасности медицинских данных, хранимых в облачной платформе в электронном виде в форме исходных физиологических сигналов (ЭЭГ, ЭКГ, ЭМГ, ЭОГ и т.д.), регистрируемых при проведении обследований пациентов; создается интегрируемая облачная платформа распределенного хранения, анализа и систематизации медицинских данных и система обеспечения безопасности с использованием разработанного метода защиты; анализируется эффективность предложенного алгоритма защиты конфиденциальной медицинской информации в условиях интеграции в разработанную облачную платформу. Предлагаемый способ защиты медицинской информационной системы подразумевает использование исходного файла формата DICOM и впоследствии преобразованного изображения в формате PNG, которое подвергается алгоритму шифрования пикселей. Для шифрования изображения применяется алгоритм на основе теории хаоса. Возможности систем хаоса позволяют значительно повысить производительность. Иерархичное разделение потоков данных на уровни и стандартизация протоколов передачи данных, а также форматов их хранения позволяют сформировать универсальную, гибкую и надежную медицинскую информационную систему. Предлагаемая архитектура имеет возможность интеграции в существующие медицинские системы. В ходе работы установлено, что рассматриваемый метод защиты является эффективным способом обеспечения конфиденциальности данных медицинской системы.

Шифрование; медицинская информационная система; конфиденциальность; облачные вычисления; информационная безопасность; обработка данных; систематизация данных; большие данные.

L.K. Babenko, A.S. Shumilin, D.M. Alekseev

ALGORITHM OF ENSURING THE SECURITY OF CONFIDENTIAL DATA OF THE MEDICAL INFORMATION SYSTEM FOR STORAGE AND PROCESSING OF EXAMINATION RESULTS

The objectives of the study are to develop and assess the effectiveness of the structure of a cloud platform for storing, processing and organizing medical data, determining a method of protection, in particular, ensuring confidentiality when transferring and storing examination results. To achieve this goal, the tasks of analyzing existing models of information processes and structures in the subject area are being solved, the features of the means for accumulating and pro-

* Работа выполнена при финансовой поддержке РФФИ в рамках проекта № 20-37-90138 – аспиранты.

cessing medical data stored in electronic information systems for patient registration, the architecture of a cloud platform for distributed data storage and an algorithm for ensuring the safety of medical data stored in the cloud are being developed. the platform in electronic form in the form of initial physiological signals (EEG, ECG, EMG, EOG, etc.) recorded during patient examinations; an integrated cloud platform for distributed storage, analysis and systematization of medical data and a security system using the developed protection method are being created; the effectiveness of the proposed algorithm for protecting confidential medical information is analyzed in the context of integration into the developed cloud platform. The proposed method for protecting a medical information system involves the use of an original DICOM file and subsequently a converted PNG image, which is subjected to a pixel encryption algorithm. An algorithm based on chaos theory is used to encrypt the image. The capabilities of chaos systems can significantly increase productivity. Hierarchical division of data streams into levels and standardization of data transfer protocols, as well as their storage formats, allow to form a universal, flexible and reliable medical information system. The proposed architecture has the ability to integrate into existing medical systems. In the course of the work, it was found that the considered protection method is an effective way to ensure the confidentiality of medical system data.

Encryption; medical information system; privacy; cloud computing; information security; data processing; systematization of data; big data.

Введение. В век всеобщей информатизации и активного развития информационных технологий медицинские учреждения в ходе выполнения диагностических исследований обрабатывают и систематизируют значительные объемы данных для последующей реабилитации и лечения пациентов. Эффективность оказываемой медицинской помощи прямо пропорциональна оперативности и удобству использования данной информации специалистами медицинских организаций. Наличие задач, связанных с хранением, систематизацией и обработкой увеличивающихся объемов данных обуславливает актуальность разработки и интеграции в медицинские учреждения медицинских информационных систем (МИС). Возможность оперирования данными в электронном виде обеспечивает оперативность получения врачом необходимой информации о пациенте, что увеличивает скорость принятия решения о постановке диагноза и методах лечения [1].

Одним из актуальных направлений в области разработки и реализации систем хранения, систематизации и обработки медицинских данных является использование возможностей облачных сервисов.

Основной целью реализации облачной платформы является создание единого информационного пространства для сбора, хранения и предоставления результатов медицинских исследований, с использованием распределенной команды квалифицированных медицинских специалистов. К категории медицинских исследований относятся результаты медицинских исследований, проведенных с использованием диагностического оборудования различных производителей.

Полученные данные могут использоваться как медицинскими учреждениями, так и научно-исследовательскими организациями. Пациент может предоставлять результаты собственных медицинских исследований другим пользователям облачной платформы или группам квалифицированных медицинских специалистов. Данные могут быть использованы медицинским персоналом, который оказывает комплекс услуг по их исследованию, анализу или экспертизе, после чего предоставляет результаты исследований.

Анализ проблемы. Медицинские организации в силу законодательства являются операторами персональных данных своих пациентов. Они принимают непосредственное участие в сборе, систематизации, накоплении, хранении, уточнении, обновлении, изменении, распространении и уничтожении такой информации.

Одной из проблем при проектировании медицинских информационных систем является необходимость интеграции механизмов защиты конфиденциальной информации. К категории конфиденциальной информации относят: фамилия, имя,

отчество пациента, месяц, дата и место рождения, серия и номер паспорта, адрес регистрации и фактического проживания, идентификационный номер налогоплательщика (ИНН), страховое свидетельство государственного пенсионного страхования (СНИЛС), семейное, социальное положение, образование, профессия, должность, специальность, серия и номер страхового медицинского полиса и его действительность и др. В связи с тем, что данная категория информации представляет собой, как правило, текстовую форму, ее защита обеспечивается стандартными методами и средствами шифрования [19, 20]. К категории персональных медицинских данных, требующих нетрадиционных подходов к их защите, относят результаты медицинских обследований пациентов, хранящихся в форме сигналов (например, сигналов электроэнцефалограммы).

Постановка задачи. В связи с тем, что требованиями законодательства установлена необходимость защиты персональных данных, ключевой задачей при реализации облачной системы хранения, систематизации и обработки медицинских данных является обеспечение безопасности хранимой информации. В рамках работы цель исследований заключается в разработке и оценке эффективности общей схемы облачной платформы, обеспечивающей выполнение определенного спектра задач, а также в выборе способа обеспечения защиты медицинских данных пациентов, в частности, обеспечения защиты результатов обследований, хранимых в электронном виде в форме сигналов ЭЭГ. **Целью работы** является повышение эффективности работы систем безопасности (блокировки злоумышленных действий) при хранении, систематизации и передаче информации в распределённых медицинских системах, имеющих облачную архитектуру.

Для достижения указанной цели в рамках работы необходимо решить следующие **задачи**:

- ♦ разработать архитектуру облачной платформы распределенного хранения данных, позволяющую взаимодействовать с различными аппаратными системами для проведения медицинских обследований;
- ♦ разработать алгоритм обеспечения безопасности медицинских данных, хранимых в облачной платформе в электронном виде в форме исходных физиологических сигналов (ЭЭГ, ЭКГ, ЭМГ, ЭОГ и т.д.), регистрируемых при проведении обследований пациентов;
- ♦ проанализировать эффективность предложенного алгоритма защиты конфиденциальной медицинской информации в условиях интеграции в разработанную облачную платформу.

Анализ современного состояния исследований. В работе [11] Котяшичев И.А. и Бырылова Е.А. рассматривают возможность использования облачных технологий с целью повышения эффективности внедрения информационных систем в различные отрасли медицины. Среди наиболее распространённых способов обеспечения безопасности данных авторы выделяют шифрование. Однако в ходе работы отмечается неотъемлемая проблема симметричных систем шифрования – проблема распределения ключей, что осложняет процесс работы с такими системами. Проблема заключается в том, что хранение ключей на облачном сервере нецелесообразно, поскольку пользователь, имеющий доступ к облачным серверам, получает доступ к ключу, а следовательно, и к расшифрованным данным.

Керейтова М.Р. и Малыш В.Н. в работе [12] отмечают проблему обеспечения информационной безопасности конфиденциальных данных пациентов как одну из наиболее важных при создании и проектировании медицинских информационных систем. Вопрос защиты информации рассматривается на примере распределенной информационной системы Департамента охраны здоровья населения Кемеровской области, охватывающей все лечебно-профилактические учреждения (ЛПУ) Кемеровской области. Авторы предлагают комплексный подход к решению проблемы:

ввести контроль за рабочими станциями на предмет необычно высокой активности, в полной мере использовать антивирусную защиту, следить за всеми обновлениями для имеющихся операционных систем, использовать многоуровневую аутентификацию пользователей, предполагающую использование USB-ключей, смарт-карт, паролей, файловых ключей. Однако предлагаемый авторами подход не учитывает механизмов обеспечения защиты данных в аспекте предотвращения их утечки и/или несанкционированного доступа при передаче и хранении информации в системах с архитектурой клиент-сервер. Таким образом, в рамках данной работы рассмотрены способы и средства, обеспечивающие защиту на уровне доступа к рабочим станциям пользователям системы, при этом не учтены

Бойченко И. В. в работе [13] отмечает важность проблемы реализации прав граждан в области защиты персональных данных пациентов. Автор рассматривает возможность использования медицинских информационно-аналитических центров в структуре здравоохранения, акцентируя внимание лишь на правовом и юридическом аспектах проблемы. Предварительный анализ, проведенный автором, позволяет сделать вывод о большом потенциале использования облачных технологий в решении задач современного здравоохранения. Однако для их повсеместного внедрения требуется грамотное техническое решение, направленное на разработку методов обеспечения безопасности передаваемой информации и конфиденциальности персональных данных пациентов.

В работе [14] Rohan Jathanna отмечает уязвимость облачных систем к атакам со стороны злоумышленников (DDoS-атаки, атаки с целью проникновения на сервер, несанкционированный доступ к базам данных). Для предотвращения потери доступа к конфиденциальным данным автор предлагает использовать возможности средств резервного копирования. Противодействие несанкционированному доступу достигается путём использования алгоритмов шифрования. Предлагаемые автором подходы имеют существенные недостатки. Система резервного копирования требует большого количества дополнительных вычислительных ресурсов и ресурсов памяти, а также обеспечения нового объекта защиты (ресурса с резервной копией). Эффективность используемых алгоритмов шифрования снижается в связи с наличием проблемы распределения ключей: необходимо предусмотреть возможность передачи ключа от клиента на сервер по защищенному каналу связи. Последствием компрометации ключа шифрования является потеря доступа к конфиденциальным данным [17].

В работе [15] Кривошеева Д.А. выделяет основные недостатки использование ассиметричных систем шифрования в медицинских облачных платформах: большие затраты вычислительных ресурсов, а также времени, которое требуется для реализации вычислительных процессов. Автор предлагает альтернативный подход к созданию симметричного ключа шифрования, основанный на использовании физиологического сигнала пациента в качестве «физиологической» подписи. Существенным недостатком предлагаемого метода является тот факт, что физиологические сигналы (электрокардиограмма, фотоплетизмограмма, электроэнцефалограмма и др.) могут изменяться в течение жизни человека. Соответственно, ключ шифрования, сформированный ранее, спустя определённое время может стать недействительным и, как следствие, доступ к персональным данным станет невозможен [16, 18].

Не менее важной проблемой предлагаемого метода видится возможность доступа к данным только со стороны их обладателя (пациента, который предоставил физиологический сигнал для формирования ключа шифрования). Таким образом, возможность получения доступа к результатам обследования другими лицами (например, лечащим доктором, родственниками пациента, аналитиком системы здравоохранения и др.) затрудняется или вовсе исключается.

Подводя итоги, стоит отметить, что в работах, доступных в открытом доступе в научной литературе и электронных библиотеках, имеются различные недостатки, основными из которых являются: проблема распределения ключей, высокие требования к вычислительным ресурсам, ресурсам времени и памяти. Предлагаемый в рамках текущего проекта подход направлен на исключение указанных выше недостатков за счет применения систем шифрования, ключевой особенностью которых является возможность реализации обработки зашифрованной информации без её расшифровки. К такой информации относятся конфиденциальные данные пациентов, представляющие собой результаты медицинских обследований, которые располагаются в глобальном хранилище на уровне хранения данных. Таким образом, появляется возможность производить вычисления с зашифрованными данными без их предварительного дешифрования.

Разработка платформы медицинской информационной системы. Для решения задачи хранения, систематизации и обработки медицинских данных разработана облачная платформа, общая схема которой представлена на рис. 1.

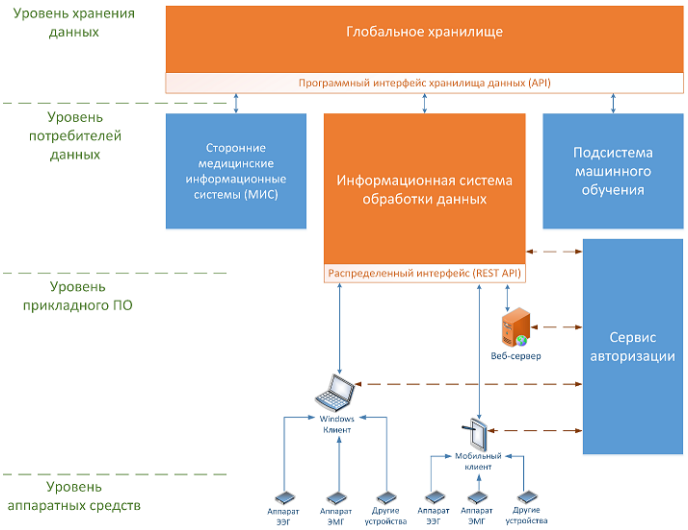

Рис. 1. Общая схема облачной платформы хранения, систематизации и обработки медицинских данных

Разработанная облачная система включает 4 основных уровня:

Уровень хранения данных: глобальное хранилище данных, которое включает в себя базу данных для хранения исходных данных обследований и отчетов, а также антропометрическая, диагностическая, демографическая информация о пациентах. Хранилище содержит полный объем информации для исследований и обучения машинных алгоритмов, но идентификация пациента возможна только по защищенному идентификатору.

Уровень потребителей данных – слой, включающий системы, которые принимают и обрабатывают данные из Глобального хранилища или передают в него новые данные. Этот уровень связан с уровнем хранения данных через стандартизированный программный интерфейс (Storage API). Потребителями данных могут быть: сторонние медицинские информационные системы; исследовательские системы; информационная система обработки данных – содержит базу персональных данных пациентов, соответствует требованиям безопасности и защиты персональных данных и медицинских данных (Федеральный закон РФ от 27 июля 2006 года

№ 152-ФЗ «О персональных данных»; Федеральный закон от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Health Insurance Portability and Accountability Act of 1996, HIPAA) [2]. Данный модуль обеспечивает взаимодействие с конечными клиентскими приложениями по средствам распределенного интерфейса (REST API).

Уровень прикладного ПО – уровень, содержащий программные средства конечных клиентов, где формируются и/или отображаются медицинские данные (обследования в виде сигналов, отчетные и персональные данные пациента): Windows клиенты – программное обеспечение для ОС семейства Windows; Вебсервер – предоставляет пользователю возможность доступа через web browser, в соответствии с назначенными этому пользователю ролями; Мобильный клиент – предоставляет доступ в информационную систему обработки данных используя мобильные устройства (Android, iOS).

Уровень аппаратных средств – физические устройства для проведения обследований. В общем случае могут быть различных видов: электроэнцефалографы, кардиографы, системы биологической обратной связи, носимые фитнес трекеры и т.д.

Экспериментальная часть. Реализация механизмов защиты при передаче данных медицинских обследований посредством облачной платформы. В ходе исследований была разработана МИС, одним из механизмов которой является обеспечение безопасности передаваемых медицинских данных. Информация, циркулирующая в системе, разделяется на два вида: текстовая информация (ФИО пациентов, паспортные данные и др.), обеспечение защиты которой достигается за счет стандартных механизмов шифрования (симметричное блочное шифрование), а также результаты медицинских обследований, хранимых в форме электроэнцефалографических сигналов. Для обеспечения защиты второй категории данных предлагается подход, основанный на конвертации исходных цифровых сигналов в формат изображений.

Разработанный механизм защиты МИС предполагает использование исходного файла DICOM и файла изображения в формате PNG, подверженного алгоритму шифрования пикселей.

Файл DICOM (Digital Imaging and Communications in Medicine) – объектно-ориентированный файл с теговой организацией: пациент → исследование → серия → изображение (кадр или серия кадров) [3, 8].

Файл содержит структурированную информацию, в том числе, медицинские изображения для их дальнейшего сохранения в виде файла PNG и данные пациента в виде текстового файла.

Предполагается использование MATLAB для извлечение медицинских изображений из файла DICOM. Язык программирования JAVA используется для исполнения кода MATLAB и для программной реализации алгоритма шифрования медицинского изображения на основе теории хаоса. Шифрование изображений предполагается выполнять на уровне прикладного ПО, непосредственно перед отправкой в глобальное хранилище. Затем зашифрованное изображение будет загружено через протокол TCP/IP в облачную систему, в которой будет храниться информация о пациенте (зашифрована с использованием блочного алгоритма шифрования) и непосредственно зашифрованное изображение в файле. Для сохранения в секрете факта передачи зашифрованной информации используются методы стеганографии.

В связи со сложной структурой файла DICOM, а также содержанием в нем разнородной информации (текст, изображение сигнала, логотип больницы, тип медицинского устройства визуализации), его обработка представляет собой сложный процесс.

Разделение файла DICOM:

Входные данные: DICOM-файл;

Выходные данные: медицинское изображение в формате .png и текстовая медицинская информация.

Шаг 1. Чтение DICOM-файла;

Шаг 2. Разделение данных пикселей медицинского изображения и связанной с ними медицинской метаинформации;

Шаг 3. Сохранение медицинской метаинформации в текстовом файле;

Шаг 4. Сохранение пикселей медицинского изображения в формате .png с 24-битной глубиной.

Таким образом, медицинское изображение будет сохранено в формате PNG в целях упрощения обработки пикселей в процессе шифрования.

Для шифрования медицинского изображения используется алгоритм на основе теории хаоса, базирующийся на традиционной криптографической архитектуре [4, 5]. Данный алгоритм, применяемый к полученному медицинскому изображению PNG, будет выполняться попиксельно: для каждого пикселя медицинского изображения.

На рис. 2 показан пример обработки медицинского изображения алгоритмом шифрования.

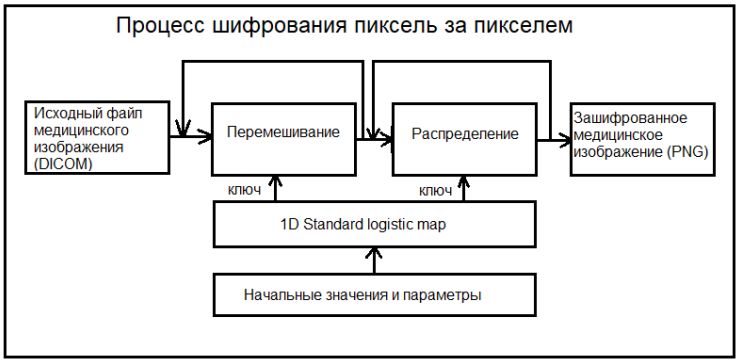

Рис. 2. Схема процесса шифрования медицинского изображения

Перемешивание пикселей означает реорганизацию расположения пикселей исходного медицинского изображения; цель шага - уменьшение высокой степени корреляции между соседними пикселями.

Следующим шагом является распределение, которое относится к изменению значений пикселей медицинского изображения путем выполнения некоторых преобразований значений пикселей. Следовательно, добавление пикселям новых значений повысит безопасность операции шифрования и отменит корреляцию между пикселями, в результате чего будет получено зашифрованное изображение с однородной гистограммой. Генератор ключей в этом процессе является одной из широко известных одномерных карт теории хаоса, известных как «1D Standard Logistic Map (SLM)» [7]. SLM имеет переменную X в качестве выходных данных, начальное условие X_n и один управляющий параметр μ, которые дают различные результаты и свойства при изменении его значения в качестве входных данных. Обычно эту карту можно описать следующим образом: $X_n + 1 = \mu X_n (1 – X_n)$ for n = 0, 1, 2, 3.

Экспериментальные результаты этой карты показывают хаотичное состояние системы, когда Xnє[0;1], управляющий параметр μє[0, 4]. Для большей точности логистическая карта всегда хаотична и имеет аппозитивный показатель Ляпунова

при 3,58≤μ≤4 [8]. В рамках работы SLM используется в качестве генератора ключей для перемешивания и распределения пикселей медицинского изображения в пространственной области, где использование SLM повторяется для всех пикселей изображения, чтобы получить произвольные значения, которые будут использоваться для шифрования пикселя [9, 10].

Шифрование медицинского изображения:

Входные данные: PNG-файл медицинского изображения;

Выходные данные: зашифрованный PNG-файл медицинского изображения.

Шаг 1. Чтение медицинского изображения и его сохранение в 2-х мерный массив пикселей;

Шаг 2. Использование стандартной логистической карты в качестве генератора случайных ключей, его начального состояния и управляющего параметра в качестве секретного ключа шифрования изображения;

Шаг 3. Перемешивание пикселей изображения (перестановка положения пикселей) в зависимости от сгенерированных значений из SLM;

Шаг 4. Распределение пикселей изображения путем изменения их значений в зависимости от ключа, сгенерированного SLM;

Шаг 5. Сохранение значения секретного ключа в том же текстовом файле, в котором хранится медицинская метаинформация, полученная из раздела DICOM-файла.

Заключение. Оценка эффективности разработанной облачной платформы хранения, систематизации и обработки медицинских данных:

Иерархичное разделение потоков данных на уровни, стандартизация протоколов передачи данных и форматов их хранения обеспечивают создание универсальной, гибкой и надежной медицинской информационной системы. Разработанная архитектура позволяет быстро интегрироваться в существующие медицинские системы. Единое пространство для хранения данных дает возможность осуществлять исследование значительного массива классифицированной медицинской информации средствами машинного обучения.

Разработанный механизм защиты МИС предполагает использование исходного файла DICOM и файла изображения в формате PNG, подверженного алгоритму шифрования пикселей. Для шифрования медицинского изображения используется алгоритм на основе теории хаоса, базирующийся на традиционной архитектуре криптографии, созданной Фридрихом. Данный алгоритм, применяемый к полученному медицинскому изображению PNG, выполняется попиксельно: для каждого пикселя медицинского изображения.

Возможности систем хаоса, которые используются для шифрования медицинских изображений, позволяют значительно повысить производительность, поскольку удовлетворяют требованиям цифровых изображений. Применение предложенного механизма шифрования медицинских данных является эффективным способом защиты информации в облачной платформе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Митькина П.А.* Особенности хранения медицинской информации // Современные научные исследования и инновации. – 2017. – № 5. – URL: http://web.snauka.ru/issues/2017/05/82546 (дата обращения: 07.10.2019).
2. Health Insurance Portability and Accountability Act. – URL: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountabilit y_Act (дата обращения: 08.10.2019).
3. DICOM. – URL: https://ru.wikipedia.org/wiki/DICOM (дата обращения 08.10.2019).
4. *L.-Y. T. a. M.-S. H. Li-Chin Huangc.* A reversible data hiding method by histogram shifting in high quality medical images // The Journals of systems and software. – 2013. – Vol. 86. – P. 716-727.

5. *M.G. a. R.D. Jessica Fridrich*, "Detecting LSB Steganography in Color and Gray-Scale Images," Binghamton.
6. *N.A. H.A.-C. Fatma E.-Z. A. Elgamal*. Secure Medical Images Sharing over Cloud Computing environment // International Journal of Advanced Computer Science and Applications. – 2013. – Vol. 4. – P. 130-138. A. B. K. R. G. a. J. P. S. Digvijay Singh Chauhan, "Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment," in 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.
7. Logistic map.– URL: https://en.wikipedia.org/wiki/Logistic_map (дата обращения 08.10.2019).
8. *Abdulrahman Alsalmany*. Cloud System for Encryption and Authentication Medical Images // IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727. – Vol. 20, Issue 1, Ver. II (Jan.-Feb. 2018). – P. 65-75. – https://www.researchgate.net/ publication/332571801_Cloud_System_For_Encryption_And_Authentication_Medical_Images (дата обращения: 29.09.2019).
9. *Плотников А.В., Прилуцкий Д.А., Селищев С.В.* Стандарт DICOM в компьютерных медицинских технологиях. – URL: https://mks.ru/library/article/1997/dicom.html (дата обращения 08.10.2019).
10. Визуальная криптография. – URL: http://cryptowiki.net/index.php?title=%D0%92%D0%B8%D0%B7%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F (дата обращения 08.10.2019).
11. *Котяшичев И.А., Бырылова Е.А*. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. – 2015. – № 6.4 (86.4). – С. 30-34. – URL: https://moluch.ru/archive/86/16357/ (дата обращения: 09.06.2020).
12. *Керейтова М.Р., Малыш В.Н.* Информационная безопасность в медицинских информационных системах // НиКа. – 2012. – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 11.06.2020).
13. *Бойченко И.В.* Построение ИТ-инфраструктуры здравоохранения на основе парадигмы облачных вычислений // Врач и информационные технологии. – 2011. – № 3. – URL: https://cyberleninka.ru/article/n/postroenie-it-infrastruktury-zdravoohraneniya-na-osnove-paradigmy-oblachnyh-vychisleniy (дата обращения: 09.06.2020).
14. *Rohan Jathanna*. Int. Journal of Engineering Research and Application www.ijera.com ISSN: 2248-9622. – June 2017. – Vol. 7, Issue 6, (Part - 5). – P. 31-38 (дата обращения: 10.06.2020).
15. *Кривошеева Дарина*. Модель угроз безопасности в системах дистанционного мониторинга состояния человека // Правовая информатика. – 2016. – № 3. – URL: https://cyberleninka.ru/article/n/model-ugroz-bezopasnosti-v-sistemah-distantsionnogo-monitoringa-sostoyaniya-cheloveka (дата обращения: 11.06.2020).
16. *Назаренко Г.И., Михеев А.Е., Горбунов П.А., Гулиев Я.И., Фохт И.А., Фохт О.А*. Особенности решения проблем информационной безопасности в медицинских информационных системах // Врач и информационные технологии. – 2007. – № 4. – URL: https://cyberleninka.ru/article/n/osobennosti-resheniya-problem-informatsionnoy-bezopasnosti-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 16.10.2020).
17. *Горбунов П.А., Фохт И.А.* Проблемы информационной безопасности в медицинских информационных системах – теоретические решения и практические разработки. Программные системы: теория и приложения / под ред. С.М. Абрамова. В 2-х т. Т. 1. – М.: Физматлит, 2006. – С. 107-112.
18. *Назаренко Г.И, Гулиев Я.И., Ермаков. Д.Е.* Медицинские информационные системы: теория и практика / под ред. Г.И. Назаренко, Г.С. Осипова. – М.: Физматлит, 2005. – 320 с.
19. *Михеев В.А.* Основы построения подсистемы защиты информации многофункциональной информационной системы // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 165-167.
20. *Клепиков Е.А., Ясько А.О.* Вопросы защиты конфиденциальной медицинской информации о пациенте в медицинских информационных системах // Символ науки. – 2016. – № 9-1. – URL: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 16.10.2020).

REFERENCES

1. *Mit'kina P.A.* Osobennosti khraneniya meditsinskoy informatsii [Features of storing medical information], *Sovremennye nauchnye issledovaniya i innovatsii* [Modern scientific research and innovations], 2017, No. 5. Available at: http://web.snauka.ru/issues/2017/05/82546 (accessed 07 October 2019).
2. Health Insurance Portability and Accountability Act. Available at: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act (accessed 08 October 2019).
3. DICOM. Available at: https://ru.wikipedia.org/wiki/DICOM (accessed 08 October 2019).
4. *L.-Y. T. a. M.-S. H. Li-Chin Huangc.* A reversible data hiding method by histogram shifting in high quality medical images, *The Journals of systems and software*, 2013, Vol. 86, pp. 716-727.
5. *M.G. a. R.D. Jessica Fridrich.* Detecting LSB Steganography in Color and Gray-Scale Images, Binghamton.
6. *N.A. H.A.-C. Fatma E.-Z. A. Elgamal*. Secure Medical Images Sharing over Cloud Computing environment, *International Journal of Advanced Computer Science and Applications*, 2013, Vol. 4, pp. 130-138. A. B. K. R. G. a. J. P. S. Digvijay Singh Chauhan, "Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment," in 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.
7. Logistic map. Available at: https://en.wikipedia.org/wiki/Logistic_map (accessed 08 October 2019).
8. *Abdulrahman Alsalmany.* Cloud System for Encryption and Authentication Medical Images, *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, p-ISSN: 2278-8727, Vol. 20, Issue 1, Ver. II (Jan.-Feb. 2018), pp. 65-75. Available at: https://www.researchgate.net/publication/332571801_Cloud_System_For_Encryption_And_Authentication_Medical_Images (accessed 29 September 2019).
9. *Plotnikov A.V., Prilutskiy D.A., Selishchev S.V.* Standart DICOM v komp'yuternykh meditsinskikh tekhnologiyakh [DICOM standard in computer medical technologies]. Available at: https://mks.ru/library/article/1997/dicom.html (accessed 08 October 2019).
10. Vizual'naya kriptografiya [Visual cryptography]. Available at: http://cryptowiki.net/index.php?title=%D0%92%D0%B8%D0%B7%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F (accessed 08 October 2019).
11. *Kotyashichev I.A., Byrylova E.A.* Zashchita informatsii v «Oblachnykh tekhnologiyakh» kak predmet natsional'noy bezopasnosti [Information protection in "Cloud technologies" as a subject of national security], *Molodoy uchenyy* [Young scientist], 2015, No. 6.4 (86.4), pp. 30-34. Available at: https://moluch.ru/archive/86/16357/ (accessed 09 June 2020).
12. *Kereytova M.R., Malysh V.N.* Informatsionnaya bezopasnost' v meditsinskikh informatsionnykh sistemakh [Information security in medical information systems], *NiKa* [NIK], 2012. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-sistemah (accessed 11 June 2020).
13. *Boychenko I.V.* Postroenie IT-infrastruktury zdravookhraneniya na osnove paradigmy oblachnykh vychisleniy [Building IT infrastructure for healthcare based on the paradigm of cloud computing], *Vrach i informatsionnye tekhnologii* [Doctor and information technologies], 2011, No. 3. Available at: https://cyberleninka.ru/article/n/postroenie-it-infrastruktury-zdravoohraneniya-na-osnove-paradigmy-oblachnyh-vychisleniy (accessed 09 June 2020).
14. *Rohan Jathanna*. Int. Journal of Engineering Research and Application www.ijera.com ISSN: 2248-9622, June 2017, Vol. 7, Issue 6, (Part - 5), pp. 31-38 (accessed 10 June 2020).
15. *Krivosheeva Darina.* Model' ugroz bezopasnosti v sistemakh distantsionnogo monitoringa sostoyaniya cheloveka [Model of security threats in systems of remote monitoring of human condition], *Pravovaya informatika* [Legal informatics], 2016, No. 3. Available at: https://cyberleninka.ru/article/n/model-ugroz-bezopasnosti-v-sistemah-distantsionnogo-monitoringa-sostoyaniya-cheloveka (accessed 11 June 2020).
16. *Nazarenko G.I., Mikheev A.E., Gorbunov P.A., Guliev Ya.I., Fokht I.A., Fokht O.A.* Osobennosti resheniya problem informatsionnoy bezopasnosti v meditsinskikh informatsionnykh sistemakh [Features of solving information security problems in medical information systems], *Vrach i informatsionnye tekhnologii* [Doctor and information technology], 2007, No. 4. Available at: https://cyberleninka.ru/article/n/osobennosti-resheniya-problem-informatsionnoy-bezopasnosti-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).

17. *Gorbunov P.A., Fokht I.A.* Problemy informatsionnoy bezopasnosti v meditsinskikh informatsionnykh sistemakh – teoreticheskie resheniya i prakticheskie razrabotki. Programmnye sistemy: teoriya i prilozheniya [Information security problems in medical information systems - theoretical solutions and practical developments. Software systems: theory and applications], ed. by S.M. Abramova. In 2nd vol. Vol. 1. Moscow: Fizmatlit, 2006, pp. 107-112.
18. *Nazarenko G.I, Guliev Ya.I., Ermakov. D.E.* Meditsinskie informatsionnye sistemy: teoriya i praktika [Medical information systems: theory and practice], ed. by G.I. Nazarenko, G.S. Osipova. Moscow: Fizmatlit, 2005, 320 p.
19. *Mikheev V.A.* Osnovy postroeniya podsistemy zashchity informatsii mnogofunktsional'noy informatsionnoy sistemy [Fundamentals of building a subsystem of information security for a multifunctional information system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 8 (85), pp. 165-167.
20. *Klepikov E.A., Yas'ko A.O.* Voprosy zashchity konfidentsial'noy meditsinskoy informatsii o patsiente v meditsinskikh informatsionnykh sistemakh [Issues of protecting confidential medical information about a patient in medical information systems], *Simvol nauki* [Symbol of Science], 2016, No. 9-1. Available at: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).

Статью рекомендовал к опубликованию д.э.н. Е.Н. Тищенко.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; 347922, г. Таганрог, ул. Чехова, 2; тел.: +79054530191; д.т.н.; профессор.

Шумилин Александр Сергеевич – e-mail: ashumilin@sfedu.ru; тел.: +79081773495; м.н.с.

Алексеев Дмитрий Михайлович – e-mail: dalekseev@sfedu.ru; тел.: +79515069532; ассистент.

Babenko Lyudmila Klimentievna – Southern Federal University; e-mail: lkbabenko@sfedu.ru, 2, Chekhov street, Taganrog, 347922, Russia; phone: +79054530191; dr. of eng. sc.; professor.

Shumilin Alexander Sergeevich – e-mail: ashumilin@sfedu.ru; phone: +79081773495; junior researcher.

Alekseev Dmitry Mikhailovich – e-mail: dalekseev@sfedu.ru; phone: +79515069532; assistant.

УДК 004.056.55 DOI 10.18522/2311-3103-2020-5-16-30

С.В. Поликарпов, В.А. Прудников, К.Е. Румянцев

ВЫЧИСЛИТЕЛЬНО ЭФФЕКТИВНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ УСРЕДНЁННЫХ ЛИНЕЙНЫХ СВОЙСТВ ПСЕВДО-ДИНАМИЧЕСКИХ ПОДСТАНОВОК

Псевдо-динамические подстановки PD-sbox могут стать эффективной заменой фиксированных подстановок в псевдо-случайных функциях, так как обладают положительными свойствами как фиксированных подстановок (малый расход вычислительных ресурсов), так и динамических подстановок (способных кардинально усложнять применение статистических методов криптоанализа). Проблемой активного внедрения псевдо-динамических подстановок является, в том числе, отсутствие вычислительно эффективного метода определения усреднённых линейных свойств для всего множества генерируемых при помощи PD-sbox эквивалентных подстановок, при этом в большинстве случаев интересует только определение максимальных значений преобладания (смещения) bias(α, β) от идеального значения 1/2. Для решения этой проблемы предлагается оригинальный метод, состоящий в том, что максимальные значения преобладания рассчитываются только для относительно небольших фиксированных подстановок, входящих в состав PD-sbox, а результирующие максимальные значения преобладания получаются путём итерационного вычисления с использованием логико-вероятностного выражения для операции Исключаю-