

УДК 61:007

DOI: 10.46548/21vek-2022-1158-0001

**БЕЗОПАСНЫЙ ОБМЕН ДАННЫМИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ
С ИСПОЛЬЗОВАНИЕМ HASBE**

© Автор(ы) 2022

SPIN: 9986-0973

AuthorID: 614496

ORCID: 0000-0002-2071-5404

ResearcherID: B-5784-2016

ScopusID: 7005080984

МИХЕЕВ Михаил Юрьевич, доктор технических наук, профессор,

заведующий кафедрой «Информационные системы и технологии»,

Пензенский государственный технологический университет

(440039, г. Пенза, проезд Байдукова/ул. Гагарина, д. 1а/11, e-mail: mix1959@gmail.com)

ORCID: 0000-0002-4130-5025

ХИЛАЛ Соня, магистрант

кафедры «Информационные системы и технологии»

Пензенский государственный технологический университет

(440039, г. Пенза, проезд Байдукова/ул. Гагарина, д. 1а/11, e-mail: sonya.nina.helal@gmail.com)

Аннотация. Облачные вычисления – это технология, которая стремительно развивается в последние годы. Она предлагает множество преимуществ, таких как неограниченное хранение данных и экономическая эффективность. Однако конфиденциальность и безопасность данных являются критическими вопросами для хранения данных в облачных вычислениях. *HASBE* (*Hierarchy Attribute Set Based Encryption*) обеспечивает хорошую масштабируемость, гибкость и контроль доступа в масштабе облачных вычислений. Он контролирует доступ к зашифрованным данным, заставляя пользователей делиться своими данными с разрешенными пользователями, контролируемые администратором домена. В данной работе основной целью является проведение сравнительного анализа основных методов безопасного обмена данными между медицинскими учреждениями, показавший перспективность подхода *EHR* на основе алгоритмов *HASBE* для повышения безопасности данных в облачных хранилищах медицинской информации. В данной статье реализована модель, которая проведет анализ и оценку производительности, чтобы показать высокую эффективность и преимущества модели.

Ключевые слова: облачные вычисления, безопасность, электронные медицинские карты, контроль доступа, безопасность данных, *HASBE*.

SECURE DATA SHARING IN CLOUD COMPUTING USING HASBE

© The Author(s) 2022

MIKHEEV Mikhail Yurievich, doctor of technical sciences, professor,

head of the department "Information Systems and Technologies"

HELAL Sonya, master's student of the department "Information Systems and Technologies"

Penza State Technological University

(440039, Penza, Baidukova Passage / Gagarina Str., 1a/11,

e-mails: mix1959@gmail.com, sonya.nina.helal@gmail.com)

Abstract. Cloud computing is a technology that has been rapidly developing in recent years. It offers many advantages, such as unlimited data storage and cost efficiency. However, data privacy and security are critical issues for data storage in cloud computing. *HASBE* (*Hierarchy Attribute Set-Based Encryption*) provides good scalability, flexibility and access control at the scale of cloud computing. It controls access to encrypted data by forcing users to share their data with authorized users controlled by the domain administrator. In this work, the main goal is to conduct a comparative analysis of the main methods to secure data exchange between medical institutions, which showed the promise of the *EHR* approach based on *HASBE* algorithms to improve data security in cloud storage of medical information. This paper implements a model that will analyze and evaluate performance to show the high performance and benefits of the model.

Keywords: cloud computing, security, electronic health records, access control, data security, *HASBE*.

Для цитирования: Михеев М.Ю. Безопасный обмен данными в облачных вычислениях с использованием *HASBE* / М.Ю. Михеев, С. Хилал // XXI век: итоги прошлого и проблемы настоящего плюс. – 2022. – Т. 11. – № 2(58). – С. 10-15. – DOI 10.46548/21vek-2022-1158-0001.

Введение. Отрасль информационных технологий арену. Облачные вычисления – одна из наиболее широко используемых компаниями технологий; она позволяет (ИТ) время от времени переводит технологии на новую

предоставлять различные услуги через Интернет. Эти ресурсы включают инструменты и приложения, такие как хранилища данных, серверы, базы данных, сети и программное обеспечение [1]. Однако с точки зрения информационной безопасности возникает несколько вопросов о различных угрозах, с которыми сталкивается облако, включая конфиденциальность пользователей и целостность хранимых данных. Чтобы обеспечить конфиденциальность и целостность данных, хранящихся в облаке, и предоставить их авторизованным пользователям. Внедрение облачных технологий растет во всех отраслях, включая здравоохранение.

Организации здравоохранения предпочитают хранить медицинскую информацию пациентов в системе учета здоровья, которая также называется *EHR* (*Electronic Health Records*). Большие данные в здравоохранении требуют инфраструктуры для лучшего хранения и управления. Доступность данных о пациентах является одной из самых насущных потребностей в секторе здравоохранения и медицины [2]. Аналогичным образом, исследователям в области здравоохранения необходим легкий доступ к большому количеству данных для проведения научного анализа. Облачные технологии применяются в таких областях здравоохранения, как мобильные приложения, порталы для пациентов, электронные медицинские карты, устройства Интернета вещей (*IoT*) и анализ больших данных [3-4]. Кроме того, использование облака в системе *EHR* применяется для улучшения медицинских услуг, упрощая доступ для пользователей, а также облегчая коммуникацию и обмен медицинскими данными между пользователями.

Конфиденциальность [5-7] используется для обеспечения защиты и безопасности личной информации пользователей. Чтобы гарантировать это, в литературе было предложено множество методов. Некоторые из них основаны на традиционных методах и алгоритмах, другие являются современными и используются в комбинации для достижения надежной защиты. Неправильное использование данных в облаке или несанкционированный доступ внешних пользователей могут представлять потенциальную угрозу. Внешние пользователи могут представлять потенциальную угрозу для хранимых данных. Люди хотят, чтобы их конфиденциальные или частные данные были доступны только уполномоченным лицам с указанными ими учетными данными. Одним из решений является применение подхода к управлению доступом на основе техники шифрования данных перед их хранением в облаке. Модель *HASBE* (*Hierarchy Attribute Set Based Encryption*) предлагает эффективное решение для обеспечения целостности данных и контроля доступа для пользователей, контролируемых администратором домена. Настоящее исследование направлено на выявление проблем безопасности и решений при внедрении облачных

вычислений в здравоохранении.

Существует несколько решений для преодоления проблем безопасности, связанных с *EHR* и системами облачных вычислений. Однако прогресс был недостаточным для удовлетворения требований безопасности федеративной среды здравоохранения (облачных вычислений) [8]. Большинство моделей информационной безопасности, разработанных до настоящего времени, были предназначены для удовлетворения требований безопасности здравоохранения в контролируемой среде, такой как база данных *EHR*, хранящаяся в больнице [9]. Текущие исследования [9] сосредоточены на шифровании и расшифровке медицинских записей в контролируемой среде без учета того, как ключи шифрования и дешифрования могут быть распределены в облаке. Традиционные механизмы управления доступом (*DAC*, *MAC* и *RBAC*) не смогли обеспечить значительную безопасность медицинских записей в облаке, поскольку обычно они используют только имя пользователя и пароль. Среда облачных вычислений представляет более сложные проблемы по сравнению с контролируемой средой (отдельное учреждение). Для усиления безопасности облака *EHR* были применены методы, основанные на шифровании и контроле доступа:

В [10] шифрование на основе атрибутов (*ABE*) не привязано к одному пользователю по сравнению с обычной криптографией с открытым ключом. Скорее, и шифротексты, и ключи пользователя связаны с набором атрибутов или политикой, если есть соответствие между ключом расшифровки и шифротекстом, только тогда происходит расшифровка шифротекста. (*ABE*) схемы состоят из двух форм, а именно, схемы шифрования атрибутов ключа-политики и схемы шифрования атрибутов шифротекста-политики. В *KP-ABE* [11] политики ассоциируются с ключами, а шифротекст – с атрибутами. Только те ключи, связанные с политикой, которая удовлетворяет атрибутам, могут расшифровать шифротекст. В *CP-ABE* [12] политики сопряжены с шифротекстом, а ключи – с атрибутами. Расшифровка происходит только в том случае, если атрибуты пользователя проходят через структуру доступа к шифротексту. Атрибутное шифрование в подходах "шифротекст-политика" все еще далеко от потребностей современных корпоративных сред. Во-первых, очень утомительно собирать "составные атрибуты", т.е. атрибуты, построенные из других атрибутов, и определять политики, использующие эти атрибуты. Во-вторых, атрибутное шифрование числовых атрибутов с поддержкой *Ciphertext-Policy* ограничено присвоением только одного значения любому данному числовому атрибуту внутри ключа. Однако мы можем решить эту проблему, задав шифрование на основе набора атрибутов политики шифротекста, которая может поддерживать составные атрибуты, гибко комбинируя различные одиночные атрибуты для формирования значимой политики, а также несколько числовых назначений для заданного

атрибута.

В [13] предложили иерархическую схему шифрования на основе набора атрибутов (*HASBE*) для контроля доступа к данным в облачных вычислениях.

Методология. *HASBE* применяется для иерархического предоставления прав пользователям, создания файлов данных, доступа к файлам, отзыва пользователей и удаления файлов. В этой схеме шифровальщик данных задает структуру доступа

к шифротексту, которая называется политикой шифротекста [13]. Расшифровать шифротекст могут только пользователи с ключами дешифрования, чьи связанные атрибуты, указанные в структуре ключей, удовлетворяют структуре доступа. Ожидается, что *HASBE* будет обладать тем же свойством безопасности, что и *CP-ABE*, безопасность которого была доказана в рамках общей модели билинейных групп и модели случайного оракула (рис. 1).

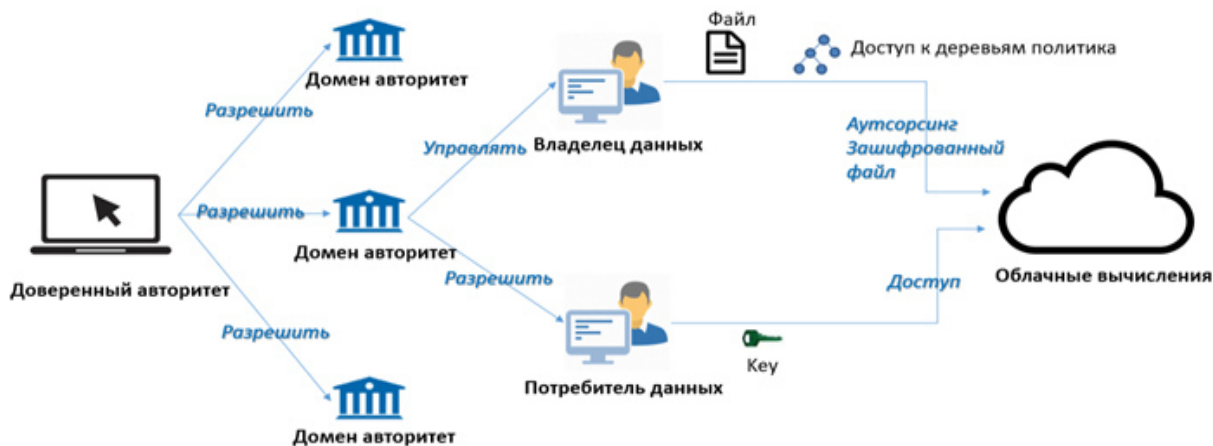


Рисунок 1 – Модель системы, реализующая алгоритм *HASBE* [13]

Общая модель безопасности описывает взаимодействие между противником и алгоритмом шифрования, таким как *HASBE* или *CP-ABE*. Идентично модели, используемой в *CP-ABE*, модель безопасности позволяет противнику запрашивать любые закрытые ключи, которые не могут быть использованы для расшифровки шифротекста вызова. В *CP-ABE* [14] шифротексты ассоциируются со структурами доступа, а закрытые ключи идентифицируются с атрибутами.

Особенности безопасности при реализации *HASBE*:

- имеет иерархическую структуру для эффективного делегирования операции генерации закрытых ключей атрибутов доверенным органом власти органам власти домена более низкого уровня. Она может обеспечить генерацию ключей атрибутов для конечных пользователей. Таким образом, эта иерархическая структура достигает большой масштабируемости;
- организует атрибуты пользователя в рекурсивную структуру множеств и позволяет пользователям накладывать динамические ограничения на то, как эти атрибуты могут быть объединены для удовлетворения политики. Таким образом, *HASBE* может поддерживать составные атрибуты и несколько числовых назначений для данного атрибута;
- обеспечивает тонкий контроль доступа. Владелец данных может быть определен и применять выразительную и гибкую политику доступа к файлам данных;
- решает проблема отзыва пользователей в облачных вычислениях.

Результаты. *HASBE* имеет инструментарий для реализации (<https://acsc.cs.utexas.edu/cpabe/>), разработанный для *CP-ABE* [15], который использует библиотеку *Pairing-Based Cryptography* (<http://crypto.stanford.edu/pbc/>). Всесторонние эксперименты проводятся на ноутбуке с двухъядерным 2,40-ГГц процессором и 8-Гб ОЗУ под управлением Ubuntu 10.04. Мы анализируем экспериментальные данные и приводим статистику. Подобно инструментарию, наш инструментарий также предоставляет несколько следующих инструментов командной строки (рис. 2):

- *hasbe-setup*: Генерирует открытый ключ и мастер-ключ;
- *hasbe-keygen*: Дает и генерирует закрытый ключ для ключевой структуры. Поддерживается ключевая структура с глубиной 1 или 2;
- *hasbe-keydel*: Дает от *DA*, делегирует некоторые части закрытых ключей *DA* новому пользователю или *DA* в своем домене. Делегированный ключ эквивалентен генерации закрытых ключей корневым органом;
- *hasbe-keyup*: Дает закрытый ключ, новый атрибут и подмножество, генерирует новый закрытый ключ, содержащий новый атрибут;
- *hasbe-enc*: Дает шифрует файл в соответствии с политикой дерева доступа, заданной на языке политик;
- *hasbe-dec*: Дать закрытый ключ и расшифровать файл;
- *hasbe-rec*: Дать закрытый ключ и зашифрованный файл, повторно зашифровать файл. Обратите внимание, что закрытый ключ должен быть способен расшифровать зашифрованный файл.

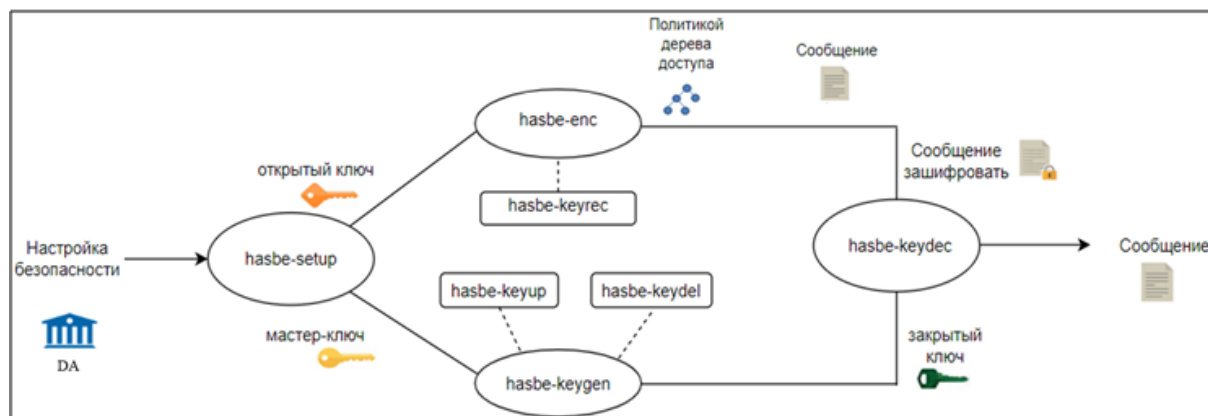


Рисунок 2 – Функции алгоритма HASBE

Облачные вычисления – это термин, используемый для описания различных типов вычислительных концепций, в которых задействовано большое количество компьютеров, соединенных сетью связи в режиме реального времени. Облачные вычисления являются синонимом распределенных вычислений по сети и означают возможность запуска программы на многих компьютерах, подключенных одновременно. Этот термин также чаще всего используется для обозначения сетевых услуг, которые предоставляются реальным серверным оборудованием, но обслуживаются виртуальным оборудованием, смоделированным программным обеспечением, работающим на одной или нескольких реальных машинах. Эти виртуальные серверы не существуют физически, поэтому их можно перемещать и увеличивать (или уменьшать) на лету, не затрагивая конечного пользователя, подобно облаку. Данные загружаются и хранятся на распределенном сервере в сети. В облачных вычислениях пользователи должны передать свои данные поставщику облачных услуг для хранения и операций, представляемых пользователями; владельцы данных шифруют свои файлы данных с помощью своего открытого ключа и хранят их на сервере для совместного использования с авторизованными потребителями данных. Для доступа к файлам данных, находящимся в общем доступе, потребители данных загружают зашифрованные файлы данных с сервера, а затем расшифровывают их с помощью своего закрытого ключа, который генерируется из их атрибутов и домена, к которому они принадлежат, где домены представляют собой отделы в системе здравоохранения. Каждый из них классифицируется в соответствии с его операционной системой, например, кардиология, неврология, гинекология и т.д.:

- создание домена: Авторизованные домены создаются для авторизованных пользователей;
- создание пользователей: Авторизованные пользователи создаются путем выделения этих Доменов;
- загрузка данных в облако: Авторизованные пользователи могут загружать свои данные в облако и просматривать опубликованные данные на облачном

сервере. Данные сначала шифруются, а затем отправляются на облачный сервер для хранения;

– пользователь-администратор: Пользователь-администратор создается для управления пользователями в Облаке. Пользователь-администратор может добавлять уровни и отменять уровень доступа пользователя;

– облачный сервер: Облачный сервер получает зашифрованный файл от отправителя данных, а также может загрузить данные пользователю. Зашифрованные файлы поступают в раздел под названием *Cloud Data publish*. На Облачном сервере;

– сервер базы данных *Hadoop*: На Облачном Сервере мы можем хранить файл на Сервере Данных *Hadoop*. *Hadoop* – это будущая система баз данных и рассматривается как сервер больших данных для растущей потребности в хранении данных.

Обсуждение. Для лучшего анализа мы сравниваем алгоритм *AES* (128 бит) и иерархическое шифрование на основе набора атрибутов по трем уровням обработки ВРЕМЯ, СТОИМОСТЬ и УРОВЕНЬ БЕЗОПАСНОСТИ.

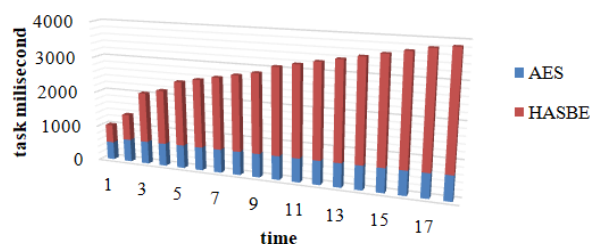


Рисунок 3 – Временная сложность для AES и HASBE

Временная сложность для алгоритма *AES* лучше, чем у *HASBE*, что, в свою очередь, свидетельствует об улучшении процессов шифрования (рис. 3). Большинство этих алгоритмов (блочные шифры *DES*, *Triple DES*, *Blowfish*) имеют сложность $O(m)O(m)$, если мы шифруем длинное сообщение, где mm – размер сообщения (табл. 1).

Безопасность является наиболее сложным аспектом облачных вычислений. Поэтому поиск оптимального решения для обеспечения жизненно важной защиты от атак злоумышленников, а также своевременное предоставление этих услуг является

одной из наиболее вдохновляющих тем в сообществах, связанных с безопасностью.

Таблица 1 – Различные параметры размера ключа

	Размер	HASBE	AES
1	128bits	0.10 sec	0.07
2	192bits	0.15 sec	0.13
3	256bits	0.18 sec	0.16

Криптография является одной из основных категорий компьютерной безопасности, которая интерпретирует информацию из ее обычной формы в нечитаемую форму. Два основных признака, которые классифицируют и отделяют один алгоритм шифрования от другого, – это его способность защитить защищаемые данные от атак, а также его скорость и эффективность при этом. В данной работе основная цель разработки любого алгоритма шифрования заключается в том, чтобы скрыть оригинал записки и отправить нестираемое текстовое сообщение получателю так, чтобы секретная передача сообщений могла происходить по сети. Стойкость алгоритма шифрования зависит от того, насколько сложно определить исходное сообщение. Было создано несколько алгоритмов шифрования с симметричным ключом, таких как *DES*, *TRIPLE DES*, *AES* и *BLOW-FISH*, чтобы обеспечить больший эффект безопасности один над другим. Хотя существующие алгоритмы разработаны по принципу *Ciphertext Policy Attribute Set Based Encryption (CP-ABE)*. Код представляет собой Иерархическую технику шифрования на основе набора атрибутов, использующую принцип *CP-ABE*. Результат анализа времени шифрования и расшифровки был более медленным, но он использует политику доступа для шифрования файлов, а для расшифровки только авторизованные пользователи могут расшифровать, что показывает, что *HASBE* имеет более высокую безопасность по сравнению с другими алгоритмами. Однако алгоритм *AES* защищен от несанкционированных атак и работает быстрее, чем популярные существующие алгоритмы (табл. 2).

Таблица 2 – Сравнение анализов Время, стоимость и безопасность

	Сложность	HASBE	AES
1	Время	Высокий	Низкий
2	Стоимость	Высокий	Низкий
3	Безопасность	Высокий	Низкий

Заметим, что *HASBE* является хорошей реализацией систем безопасности в облачных вычислениях. Среди его основных достоинств следует указать следующие возможности:

- использования для хранения больших файлов баз данных с применением технологии *Big Data*;
- использования в качестве узкоспециализированного доступа для чувствительных файлов баз данных, таких как медицина, а также других, таких как военные и банковские базы данных;
- обеспечения масштабируемого гибкого контроля доступа для различных доменов;

– применения во всех видах архитектуры для облачных вычислений.

Выводы. Организации здравоохранения в глобальном мире предполагают обмен медицинской информацией в рамках глобальных медицинских информационных систем, и такая консолидация медицинской информации важна не только с точки зрения предотвращения пандемий и других глобальных процессов, но и оказывается одной из важнейших целей для злоумышленников. В статье проведен сравнительный анализ основных методов безопасного обмена данными между медицинскими учреждениями, показавший перспективность подхода *EHR* на основе алгоритмов *HASBE*, который позволил реализовать масштабируемый, гибкий контроль доступа в облачных хранилищах медицинской информации. Использование *AES* могло бы быть более быстрым, надежным и наиболее полезным для защиты данных, однако алгоритм *HASBE* органично вписывается в иерархическую структуру пользователей системы и обеспечивает эффективное разграничение прав пользователей за счет множественного присвоения значений атрибутов. При этом система хранения медицинской информации остается гибкой даже в условиях безопасности в облачной среде, но ряд частных вопросов ее применения в глобальном информационном пространстве требует дальнейшего исследования и развития.

СПИСОК ЛИТЕРАТУРЫ:

1. Julian Araujo, Paulo Maciel, Ermeson Andrade, Gustavo Callou, Vandi Alves & Paulo Cunha. Decision making in cloud environments: an approach based on multiple-criteria decision analysis and stochastic models. *Journal of Cloud Computing*, 2–4 March 2018; pp. 2–5.
2. Yao Q, Han X, Ma XK, Xue YF, Chen YJ, Li JS. Cloud-based hospital information system as a service for grassroots health-care institutions. *Journal of medical systems*. 2014;38(9):104.
3. Farahnaz S. Rania Fahim E. Leila E. Abbas S. *Frontiers in Health Informatics* How the health information systems can overcome the challenges of migrating to the cloud? A framework based on a mix method approach. February 2022 DOI:10.30699/fhi.v10i1.342.
4. Madanian S, Parry D. IoT, Cloud Computing and Big Data: Integrated Framework for Healthcare in Disasters. *Studies in health technology and informatics*. 2019;264:998–1002.
5. Guilloteau S., Venkatesen M. Privacy in Cloud Computing-ITU-T Technology Watch Teport March 2012. International Telecommunication Union; Geneva, Switzerland: 2013.
6. Cook A., Robinson M., Ferrag M.A., Maglaras L.A., He Y., Jones K., Janicke H. *Cloud Computing for Optimization: Foundations, Applications, and Challenges*. Springer; Berlin/Heidelberg, Germany: 2018. Internet of Cloud: Security and Privacy Issues; pp. 271–301.
7. Xiao Z., Xiao Y. Security and Privacy in Cloud Computing. *IEEE Commun. Surv. Tutor*. 2013;15:843–859. doi: 10.1109/SURV.2012.060912.00182.
8. Mahmood GS, Huang Dong Jun, Jaleel BA. 2019, “A Secure Cloud Computing System by Using Encryption and Access Control Model”.
9. J Healthc Eng. eHealth Cloud Security Challenges: A Survey. 2019; 2019: 7516035. Published online 2019 Sep 3. doi: 10.1155/2019/7516035.
10. Begam BF, Sasiskala M. Attribute-based Encryption in Cloud Computing – A Review. *International Journal of Computer Applications*. 2021;174(19):36-38. doi:10.5120/ijca2021921084.
11. Yinghui z. Robert h. D. Shengmin x. Jianfei s. Qi l. Dong z. Attribute-based Encryption for Cloud Computing Access Con-

trol: A Survey. Published in ACM Computing Surveys, September 2020, 53 (4), Article number 3398036 DOI: 10.1145/3398036.

12. Helil N, Rahman K. CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy. Security and Communication Networks. 2017;2017. doi:10.1155/2017/2713595.

13. Wan Z, Liu J, Deng RH. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics and Security. 2012;7(2):743-754. doi:10.1109/TIFS.2011.2172209.

14. Lai J., Deng R.H., Li Y. Expressive CP-ABE with partially hidden access structures; Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security; Seoul, Korea. 2021(1):1-16 DOI:10.1155/2021/4132597.

15. Jayapandian N, Rahman AMJZ. Secure Wireless Cloud Data Storage using Hierarchical-Attribute-based Encryption with Identity Based Encryption. Asian Journal of Research in Social Sciences and Humanities. 2017;7(1):1000. doi:10.5958/2249-7315.2017.00038.7.

Статья поступила в редакцию 10.05.2022

Статья принята к публикации 20.06.2022