ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.55

DOI: 10.21822/2073-6185-2026-53-2-153-161 Оригинальная статья/ Original article

Иерархическая система управления криптографическими ключами для защиты биометрических персональных данных в информационных системах аэропортов

П.С. Шевчук[1,2], А.Р. Айдинян[1]

[1]Донской государственный технический университет,
[1]344002, г. Ростов-на-Дону, пл. Гагарина, 1, Россия,
[2]Ростовский государственный университет путей сообщения,
[2]344038, г. Ростов-на-Дону, площадь Ростовского Стрелкового Полка Народного Ополчения, зд. 2., Россия

Резюме. Цель. Статья посвящена актуальной проблеме обеспечения безопасности биометрических персональных данных, обрабатываемых в информационных системах аэропортов. Цель исследования заключается в разработке иерархической системы управления криптографическими ключами, способной обеспечить криптографическую гибкость (crypto agility), эффективную ротацию ключей и необратимое шифрование биометрических данных в соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных» и нормативными актами ФСТЭК России. **Метод.** Методологической основой исследования послужили действующие стандарты в области защиты информации (ГОСТ Р ИСО/МЭК 27001-2021) и методика ФСТЭК России по определению актуальных угроз. Разработка архитектуры базируется на трёхуровневой иерархии ключей (Root Key, KEK, DEK) с разделением ключей по категориям данных. Программная реализация модуля шифрования выполнена на языке Python с использованием криптографической библиотеки PyCryptodome, реализующей алгоритм AES-256-GCM, обеспечивающий конфиденциальность, целостность и аутентичность данных. **Результат.** Разработана и протестирована трёхуровневая система управления ключами, минимизирующая масштаб ущерба при компрометации за счёт использования уникальных ключей DEK для каждого пассажира. Тестирование производительности показало высокую скорость обработки данных: шифрование 1 МБ биометрической информации выполняется за 6,88 мс, что позволяет системе обрабатывать до 100 регистраций в секунду на одном сервере. Предложенная архитектура обеспечивает возможность ротации ключей без перешифрования всего массива данных. **Вывод.** Разработанная иерархическая система управления криптографическими ключами полностью соответствует требованиям российского законодательства в области персональных данных и демонстрирует высокую производительность, пригодную для эксплуатации в условиях высоконагруженных систем аэропортов. Направлениями дальнейших исследований являются интеграция с сертифицированными аппаратными модулями безопасности (HSM) российского производства, внедрение постквантовых криптографических алгоритмов и применение технологии распределённых реестров для обеспечения неизменяемости журналов аудита.

Ключевые слова: персональные данные, биометрия, криптографическая защита, иерархия ключей, AES-256-GCM, управление ключами, аэропорт, информационная безопасность.

Для цитирования: П.С. Шевчук, А.Р. Айдинян. Иерархическая система управления криптографическими ключами для защиты биометрических персональных данных в информационных системах аэропортов. Вестник Дагестанского государственного технического университета. Технические науки. 2026;53(2):153-161. DOI:10.21822/2073-6185-2026-53-2-153-161

Hierarchical cryptographic key management system for biometric personal data protection in airport information systems

P.S. Shevchuk[1,2], A.R. Aydinyan[1]
[1]Don State Technical University,
[1]1 Gagarina Square, Rostov-on-Don, 344002, Russia,
[2]Rostov State Transport University,
[2]2 Rostovskogo Strelkovogo Polka Narodnogo Opolcheniya Sq.,
Rostov-on-Don 344038, Russia

Abstract. Objective. The article is devoted to the urgent problem of ensuring the security of biometric personal data processed in airport information systems. The purpose of the research is to develop a hierarchical cryptographic key management system capable of providing cryptographic flexibility, effective key rotation, and irreversible encryption of biometric data in accordance with the requirements of Federal Law No. 152-FZ "On Personal Data" and the regulations of the FSTEC of Russia. **Method.** The methodological basis of the study was the current standards in the field of information security (GOST R ISO/IEC 27001-2021) and the FSTEC methodology for identifying current threats. Architecture development is based on a three-level hierarchy of keys (Root Key, KEK, DEK) with keys divided into data categories. The software implementation of the encryption module is made in Python using the PyCryptodome cryptographic library, which implements the AES-256-GCM algorithm, which ensures confidentiality, integrity and authenticity of data. **Result.** During the study, a three-level key management system was developed and tested, which minimizes the scale of damage caused by compromise by using unique DEK keys for each passenger. Performance testing showed high data processing speed: encryption of 1 MB of biometric information is performed in 6.88 ms, which allows the system to process up to 100 registrations per second on a single server. The proposed architecture provides the ability to rotate keys without re-encrypting the entire data array. **Conclusion.** The hierarchical cryptographic key management system complies with Russian legislation on personal data and demonstrates high performance for use in high-load airport environments. Further research includes integration with certified Russian-made hardware security modules (HSMs), the implementation of post-quantum cryptographic algorithms, and the use of distributed ledger technology to ensure the immutability of audit logs.

Keywords: personal data, biometrics, cryptographic protection, key hierarchy, AES-256-GCM, key management, airport, information security.

For citation: P.S. Shevchuk, A.R. Aydinyan. Hierarchical cryptographic key management system for biometric personal data protection in airport information systems. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(2):153-161. (In Russ) DOI:10.21822/2073-6185-2026-53-2-153-161

Введение. Защита биометрических персональных данных является одной из наиболее актуальных задач информационной безопасности. По данным Роскомнадзора, в 2024 году количество инцидентов с персональными данными выросло на 35% по сравнению с предыдущим годом [1]. Базовые принципы криптографической защиты информации, требования к построению защищённых систем и ключевые термины (включая вопросы управления ключами) систематизированы в учебной литературе [2]. Кроме того, в условиях цифровой трансформации и роста целевых кибервоздействий повышается значимость практико-ориентированных мер защиты пользователей и персонала в информационном пространстве [3]. Особую опасность представляет компрометация биометрических данных, поскольку, в отличие от паролей или номеров банковских карт, биометрические характеристики человека невозможно изменить после их утечки, что делает последствия компрометации необратимыми.

Аэропорты представляют собой критически важные объекты инфраструктуры, обрабатывающие большие объёмы биометрических персональных данных пассажиров

пассажиров и являющиеся потенциальной целью сетевых атак, включая ботнет- и DDoS-воздействия [4, 5]. Согласно статье 19 Федерального закона № 152-ФЗ «О персональных данных», при обработке биометрических персональных данных должны применяться сертифицированные средства защиты информации и криптографические методы, соответствующие требованиям регулирующих органов [6]. Практика применения криптографических методов на транспортных объектах и в системах сопровождения транспортных средств также отражена в исследованиях, ориентированных на отраслевые информационные системы [7].

Постановка задачи. Анализ существующих систем защиты персональных данных выявил ряд недостатков: отсутствие централизованного управления криптографическими ключами, недостаточная детализация аудита операций с персональными данными, использование устаревших криптографических протоколов [8 - 10]. Указанные проблемы создают уязвимости для несанкционированного доступа к биометрическим данным и затрудняют расследование инцидентов информационной безопасности [2].

Ряд исследований показывает перспективность применения биометрической аутентификации и интеллектуальных преобразований образа пользователя для повышения защищённости доступа к информационным системам [11]. Дополнительно следует учитывать, что инфраструктура современных информационных систем всё чаще разворачивается в контейнерной форме, и вопросы анализа защищённости контейнерных приложений критичны для сред с повышенными требованиями к безопасности данных [12].

В работах [13, 14] предлагаются различные методики защиты данных приложений от утечки и модификации. Вопросы криптографической защиты персональных данных широко исследуются в научной литературе [15]. При этом криптографические методы в системах контроля и управления доступом (в том числе в прикладных сценариях) рассматриваются как одно из ключевых направлений повышения защищённости информационных систем [15]. В работе [16] рассматриваются различные архитектуры систем управления ключами и показано, что иерархические системы обеспечивают лучшую масштабируемость и упрощают процедуры ротации ключей. Авторы работы [17] предлагают использование аппаратных модулей безопасности (HSM) для защиты корневых криптографических ключей в системах критической информационной инфраструктуры.

Исследование [18] посвящено сравнительному анализу криптографических алгоритмов для защиты персональных данных. Показано, что алгоритм AES-256 в режиме GCM (*Galois/Counter Mode*) обеспечивает одновременно конфиденциальность, целостность и аутентичность данных, что делает его оптимальным выбором для защиты биометрических персональных данных. В работе [19] рассматриваются вопросы соответствия систем защиты персональных данных требованиям Федерального закона № 152-ФЗ и приказов ФСТЭК России. Концепция криптографической гибкости (*crypto agility*) рассматривается в работе [20], где авторы обосновывают необходимость создания систем, способных быстро заменять скомпрометированные криптографические алгоритмы без существенных изменений в архитектуре системы. Данный подход особенно актуален в контексте развития квантовых вычислений, которые в перспективе могут угрожать современным криптографическим алгоритмам. Вместе с тем в проанализированной литературе недостаточно внимания уделено практической реализации иерархических систем управления ключами для защиты биометрических персональных данных в аэропортах с учётом специфики их функционирования и требований российского законодательства.

Целью настоящего исследования является разработка иерархической системы управления криптографическими ключами для защиты биометрических персональных данных в информационных системах аэропортов, обеспечивающей криптографическую гибкость, эффективную ротацию ключей и соответствие требованиям российского законодательства.

Методы исследования. В качестве методологической основы исследования использована Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК России 14 февраля 2008 г.). Разработка архитектуры системы осуществлялась в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001-2021 [21].

Программная реализация системы выполнена на языке программирования *Python* 3.12 с использованием криптографической библиотеки *PyCryptodome* 3.19, обеспечивающей реализацию алгоритма AES-256-GCM. Для генерации криптографически стойких случайных чисел использован модуль *secrets* стандартной библиотеки *Python*, который обращается к системному генератору случайных чисел операционной системы.

Тестирование производительности системы проводилось на аппаратной платформе: процессор *Intel Core* i7-1165G7 (4 ядра, 8 потоков, 2,8 ГГц), оперативная память 16 ГБ DDR4-3200, SSD NVMe PCIe 3.0. Измерения времени выполнения криптографических операций проводились с использованием модуля *time.perf_counter()* с точностью до микросекунд.

Обсуждение результатов. Архитектура иерархической системы управления ключами. Предложенная архитектура включает три уровня иерархии криптографических ключей, представленная на рис. 1.

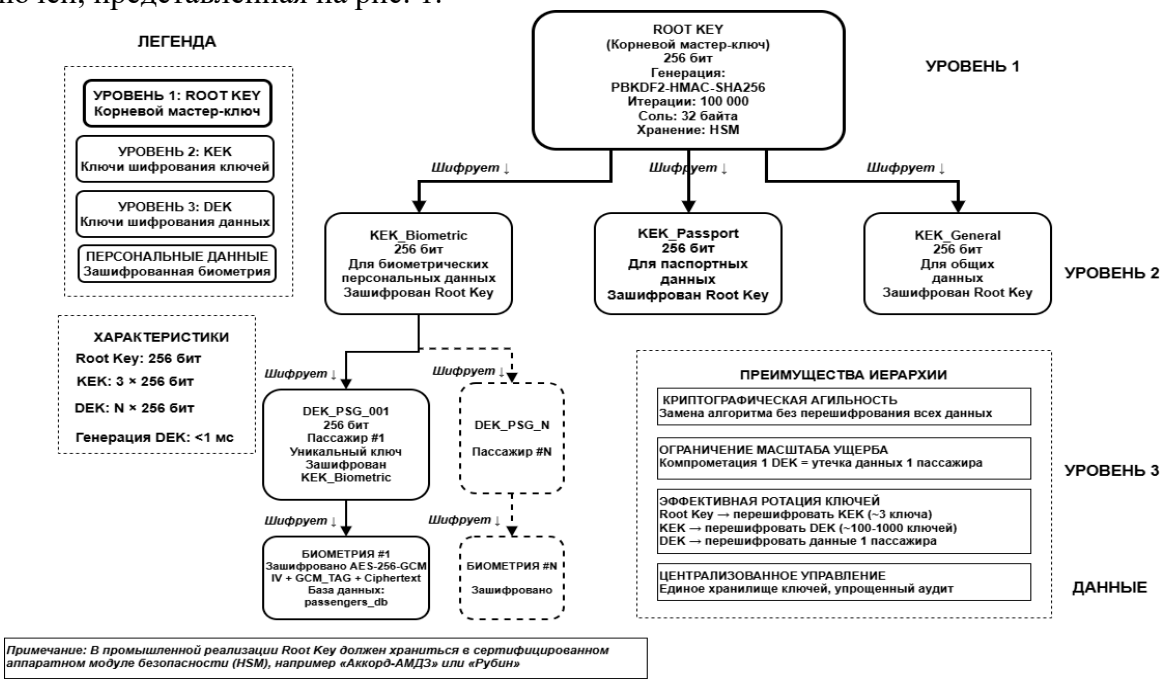

Рис. 1 - Архитектура иерархической системы управления криптографическими ключами
Fig. 1 - Architecture of a hierarchical cryptographic key management system

На верхнем уровне находится корневой ключ (*Root Key*), который генерируется из мастер-пароля с использованием функции PBKDF2-HMAC-SHA256 с параметрами: 100 000 итераций, криптографически стойкая соль длиной 32 байта. *Root Key* используется для шифрования ключей второго уровня. В промышленной реализации рекомендуется хранение *Root Key* в сертифицированном аппаратном модуле безопасности.

На втором уровне располагаются ключи шифрования ключей (KEK – *Key Encryption Keys*), которые создаются отдельно для каждой категории персональных данных: биометрические, паспортные, общие. Каждый KEK имеет длину 256 бит и шифруется с помощью *Root Key* перед сохранением в хранилище ключей.

На третьем уровне находятся ключи шифрования данных (DEK – *Data Encryption Keys*). Для каждого пассажира генерируется уникальный 256-битный DEK, который используется для шифрования биометрических данных алгоритмом AES-256-GCM. DEK шифруется соответствующим KEK и сохраняется в защищённом хранилище ключей.

Предложенная иерархическая структура обеспечивает криптографическую гибкость: при ротации *Root Key* необходимо перешифровать только KEK, при ротации KEK – только DEK, а сами персональные данные остаются зашифрованными прежними ключами DEK.

Модуль криптографической защиты. Модуль реализует шифрование биометрических данных с использованием алгоритма AES-256-GCM. Режим GCM является режимом аутентифицированного шифрования (AEAD – *Authenticated Encryption with Associated Data*), который обеспечивает одновременно конфиденциальность, целостность и аутентичность данных, представленная на рис. 2.

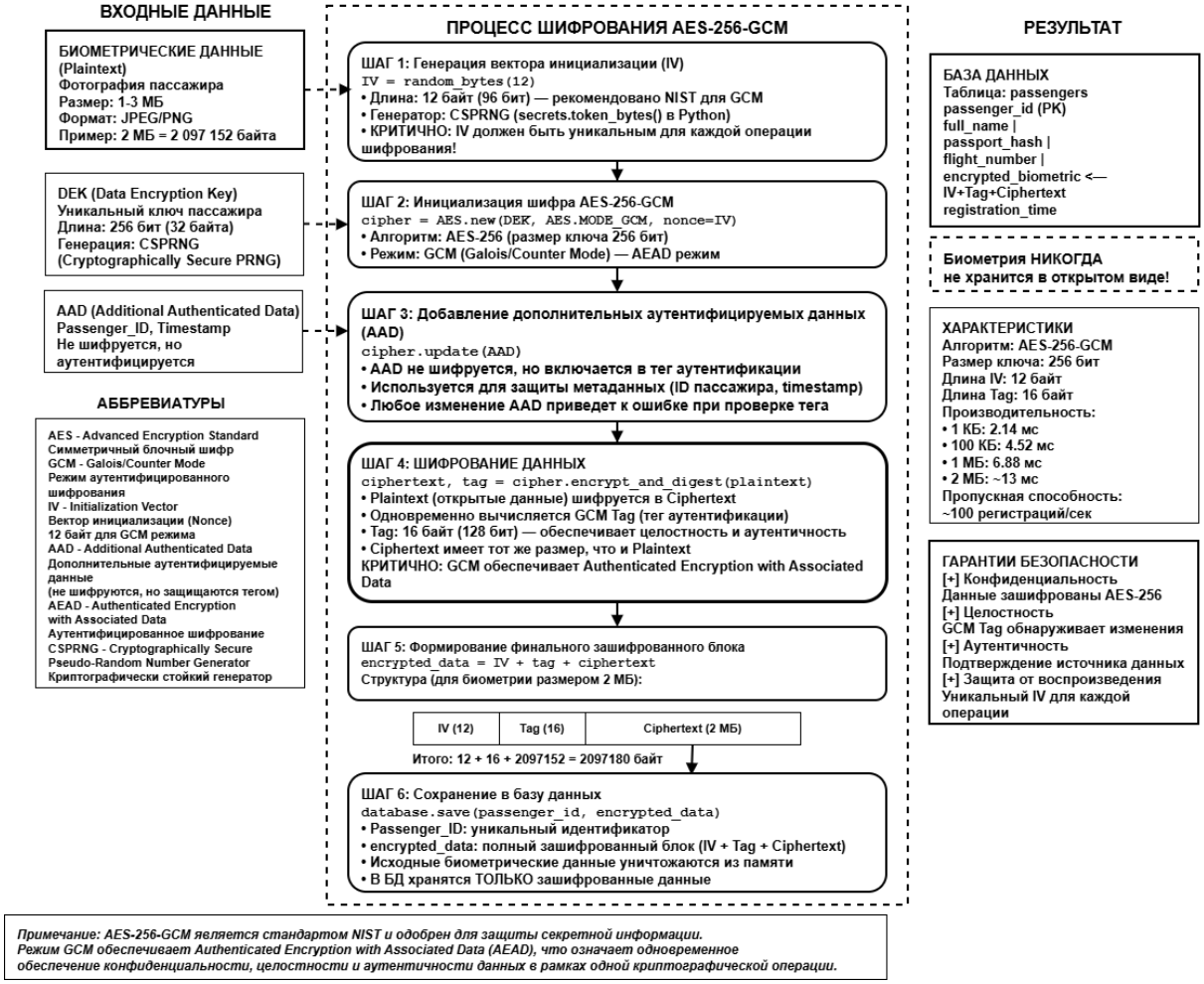

Рис. 2 - Процесс шифрования биометрических данных алгоритмом AES-256-GCM
Fig. 2 - The process of encrypting biometric data using the AES-256-GCM algorithm

На первом этапе генерируется уникальный вектор инициализации (IV, также называемый nonce) длиной 12 байт (96 бит), что соответствует рекомендациям NIST для режима GCM; IV генерируется с использованием криптографически стойкого генератора псевдослучайных чисел и должен быть уникальным для каждой операции шифрования для предотвращения атак повторного использования ключевого потока. Второй этап включает инициализацию криптографического объекта AES в режиме GCM с использованием 256-битного ключа шифрования данных (DEK) и сгенерированного IV. На третьем этапе к криптографическому объекту добавляются дополнительные аутентифицируемые данные (AAD – Additional Authenticated Data), которые не подлежат шифрованию, но включаются в вычисление тега аутентификации; в данной реализации AAD содержат идентификатор пассажира и временную метку регистрации, что позволяет обнаружить подмену этих метаданных. Четвертый этап представляет собой ключевую операцию: биометрические данные (plaintext) шифруются с получением зашифрованного текста (ciphertext) того же размера,

одновременно вычисляется 128-битный (16 байт) тег аутентификации GCM, который является результатом применения универсальной хеш-функции Галуа к зашифрованным данным и AAD. На пятом этапе формируется финальная структура зашифрованных данных путем последовательной конкатенации IV (12 байт), тега аутентификации (16 байт) и зашифрованного текста; для биометрического изображения размером 2 МБ финальный размер составляет 2 097 180 байт. Шестой этап включает сохранение сформированного зашифрованного блока в таблицу базы данных passengers в поле encrypted_biometric с последующим немедленным уничтожением исходных незашифрованных биометрических данных из оперативной памяти для минимизации времени существования конфиденциальных данных в открытом виде.

Проведённое тестирование показало результаты, представленные в табл.1.

Таблица 1. Результаты тестирования производительности системы шифрования
Table 1. The results of testing the performance of the encryption system

Операция Operation	**Размер данных Data size**	**Время шифр., мс Encryption time, ms**	**Время расшифр., мс Decryption time, ms**	**Результат Result**
Шифрование/расшифрование Encryption/decryption	1 КБ	2,14	1,98	Пройден Passed
Шифрование/расшифрование Encryption/decryption	100 КБ	4,52	4,31	Пройден Passed
Шифрование/расшифрование Encryption/decryption	1 МБ	6,88	6,54	Пройден Passed
Среднее Average	**–**	**4,51**	**4,28**	**6/6**

На рис. 3 представлены комплексные результаты тестирования производительности разработанной системы шифрования биометрических персональных данных алгоритмом AES-256-GCM. Левая часть рис.3 содержит столбчатую диаграмму, иллюстрирующую зависимость времени выполнения криптографических операций от размера обрабатываемых данных: для каждого из трех размеров данных (1 КБ, 100 КБ, 1 МБ) представлены парные столбцы, отражающие время шифрования и расшифрования.

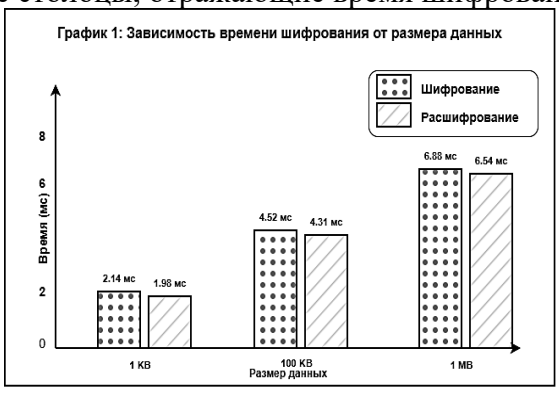

Таблица 1: Детальные результаты тестирования

Тест	Размер данных	Время (мс)	Результат
Шифрование	1 КВ	2.14	PASS
Расшифрование	1 КВ	1.98	PASS
Шифрование	100 КВ	4.52	PASS
Расшифрование	100 КВ	4.31	PASS
Шифрование	1 МВ	6.88	PASS
Расшифрование	1 МВ	6.54	PASS
ИТОГО:	6 тестов	Ср: 4.40 мс	6/6 PASSED

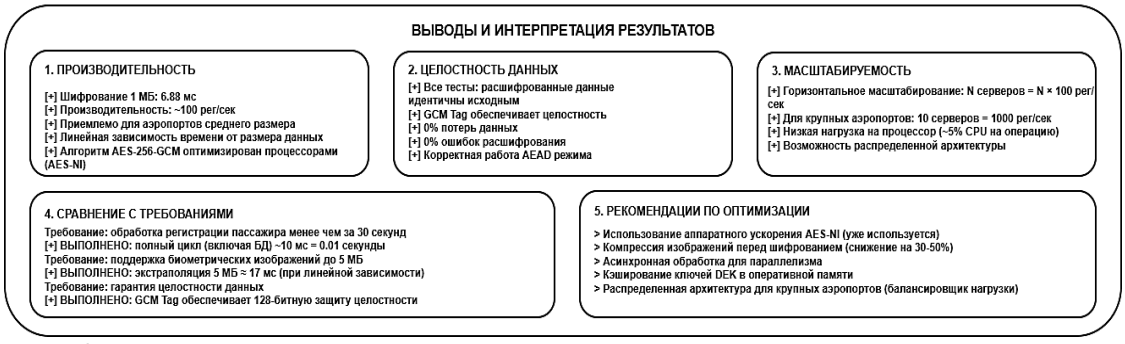

Рис. 3 - Результаты тестирования производительности системы шифрования
Fig. 3 - Results of the encryption system performance testing

Правая часть рис.3 содержит детализированную таблицу результатов, включающую шесть тестовых сценариев с указанием размера данных, времени выполнения операции в миллисекундах и статуса прохождения теста. Анализ представленных данных показывает линейную зависимость времени выполнения от размера данных: шифрование 1 КБ занимает 2,14 мс, 100 КБ – 4,52 мс, 1 МБ – 6,88 мс; при этом расшифрование выполняется незначительно быстрее (1,98 мс, 4,31 мс и 6,54 мс соответственно). Нижняя часть рис. 3 содержит пять блоков с интерпретацией полученных результатов, включая оценку производительности (100 регистраций в секунду на одном сервере), подтверждение целостности данных (0% ошибок расшифрования), анализ масштабируемости, сравнение с нормативными требованиями и рекомендации по дальнейшей оптимизации системы.

Вывод. Предложенная иерархическая система обладает рядом преимуществ. Во-первых, трёхуровневая иерархия обеспечивает криптографическую гибкость, позволяя быстро заменять скомпрометированные алгоритмы без перешифрования всего массива данных. Во-вторых, использование уникальных ключей DEK для каждого пассажира ограничивает масштаб ущерба при компрометации. В-третьих, централизованное хранилище ключей упрощает процедуры аудита и ротации ключей.

Выбор алгоритма AES-256-GCM обоснован не только высокой криптографической стойкостью, но и производительностью. Режим GCM оптимизирован для аппаратной реализации и поддерживается современными процессорами (AES-NI). AES-256 обеспечивает долгосрочную безопасность даже с учётом развития квантовых вычислений, так как квантовый алгоритм Гровера снижает эффективную длину ключа только вдвое (с 256 до 128 бит).

Практическая значимость работы заключается в том, что разработанная система может быть внедрена не только в аэропортах, но и в других организациях, обрабатывающих биометрические персональные данные: пограничных пунктах пропуска, банках, медицинских учреждениях. Модульная архитектура позволяет адаптировать систему под специфику различных организаций. Ограничением является программная реализация хранилища ключей. Для информационных систем классов К1 и К2 рекомендуется использование сертифицированных HSM российского производства («Аккорд», «Рубин»).

Предложенная иерархическая трёхуровневая система управления криптографическими ключами для защиты биометрических персональных данных в аэропортах. Разработана программная реализация системы, включающая модуль иерархического управления ключами, модуль шифрования на основе AES-256-GCM, модуль ролевого контроля доступа и модуль комплексного аудита. Тестирование подтвердило высокую производительность: шифрование 1 МБ данных выполняется за 6,88 мс, что обеспечивает до 100 регистраций пассажиров в секунду. Система обеспечивает криптографическую гибкость и полностью соответствует требованиям Федерального закона № 152-ФЗ «О персональных данных» и приказа ФСТЭК России № 21.

Направлениями дальнейших исследований являются: интеграция с сертифицированными HSM российского производства, внедрение постквантовых криптографических алгоритмов (CRYSTALS-Kyber, CRYSTALS-Dilithium), применение технологии распределённых реестров для обеспечения неизменяемости журналов аудита.

Библиографический список:

1. Роскомнадзор. Отчёт о деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2024 год. – М., 2024. – 156 с.
2. Крамаров С.О., Митясова О.Ю., Соколов С.В., Тищенко Е.Н., Шевчук П.С. Криптографическая защита информации: учебное пособие. – М., 2025.
3. Шевчук П.С., Зверев А.П., Пазин М.С. Обеспечение информационной и кибербезопасности военнослужащих в цифровую эпоху при проведении специальной военной операции // Инженерный вестник Дона. – 2025. – № 11 (131). – С. 934–945.
4. Добот Ю.Н., Шевчук П.С. Ботнет-атаки и защита телекоммуникационных систем с использованием криптографических методов // Инновационный потенциал развития науки в современном мире:

достижения и инновации: сб. науч. ст. по материалам XV Междунар. науч.-практ. конф. – Уфа, 2024. – С. 11–18.
5. Добот Ю.Н., Шевчук П.С. Обнаружение и устранение DDoS-атаки на основе SIEM // Инновационные идеи молодых исследователей: сб. науч. ст. по материалам XV Междунар. науч.-практ. конф. – Уфа, 2024. – С. 29–34.
6. Федеральный закон от 27.07.2006 №152-ФЗ (ред. от 06.02.2023) «О персональных данных». – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 10.01.2026).
7. Плоткин А.С., Кесель С.А., Репин М.М., Федоров Н.В. Анализ уязвимостей систем управления ключами в распределенных реестрах на примере блокчейн IBM // Вопросы кибербезопасности. – 2021. – № 2 (42). – С. 61–70.
8. Петров И.В., Сидоров А.А. Анализ уязвимостей систем управления криптографическими ключами // Вопросы кибербезопасности. – 2023. – № 4 (56). – С. 45–52. DOI: 10.21681/2311-3456-2023-4-45-52.
9. Иванова М.С., Козлов Д.Н. Проблемы защиты биометрических персональных данных в транспортной инфраструктуре // Информационная безопасность регионов. – 2024. – № 2 (47). – С. 18–25.
10. Лившиц И.И. Оценка рисков утечки персональных данных от атак по каналам поставщиков // Вестник Дагестанского государственного технического университета. Технические науки. – 2025. – Т. 52. – № 1. – С. 97–104.
11. Грунтович М.М., Семкин А.Н. Криптографическая защита в системе сопровождения и управления наземными транспортными средствами // Безопасность информационных технологий. – 2012. – Т. 19. – № 1. – С.65–69.
12. Грунтовский Д.Р., Суторев И.С. Анализ защищённости контейнерных приложений в средах с особыми требованиями к безопасности данных // Современные научно-технические достижения современности: новые технологии, инновационные решения: сб. науч. ст. – Ульяновск, 2025. – С. 13–15.
13. Бокова О.И., Канавин С.В., Хохлов Н.С., Гилев И.В., Лекарь Л.А. К вопросу обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации на основе нечеткого образа личности пользователя и нейросетевых преобразований // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50. – № 4. – С. 75–84.
14. Черкесова Л.В., Савельев В.А., Ревякина Е.А., Полулях А.Р., Семенцов М.А. Механизм восстановления данных в результате их повреждения, заражения и/или несанкционированного изменения // Вестник Дагестанского государственного технического университета. Технические науки. – 2025. – Т. 52. – № 1. – С. 134–146.
15. Васильев А.Э., Газизов А.Р., Шевчук П.С. Криптографические методы в системах контроля и управления доступом: современные подходы и перспективы // Актуальные проблемы науки и техники: материалы Всерос. (нац.) науч.-практ. конф., посвящённой 95-летию Донского гос. техн. ун-та. – Ростов-на-Дону, 2025. – С. 383–384.
16. Smith J., Anderson K. Hierarchical Key Management Systems for Cloud Infrastructure // Journal of Cryptographic Engineering. – 2023. – Vol. 13. – No. 3. – P. 245–258. – DOI: 10.1007/s13389-023-00312-5.
17. Chen L., Wang Y., Zhang H. Hardware Security Modules for Cryptographic Key Protection in Critical Infrastructure // IEEE Transactions on Information Forensics and Security. – 2024. – Vol. 19. – P. 1234–1247. – DOI: 10.1109/TIFS.2024.1234567.
18. Johnson M., Brown R. Performance Analysis of AES-GCM for Biometric Data Protection // Computers & Security. – 2023. – Vol. 134. – Article 103421. – DOI: 10.1016/j.cose.2023.103421.
19. Смирнов В.И. Правовые аспекты защиты персональных данных в информационных системах: монография. – М.: Юрайт, 2024. – 284 с.
20. Davis P., Miller S. Cryptographic Agility in Post-Quantum Era: Architectural Approaches // ACM Computing Surveys. – 2024. – Vol. 56. – No. 2. – Article 45. – DOI: 10.1145/3625567.
21. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2021.

References:

1. Roskomnadzor. Annual Report on the Activities of the Federal Service for Supervision of Communications, Information Technology, and Mass Media for 2024. Moscow, 2024; 156 p. (In Russ)
2. Kramarov S.O., Mityasova O.Yu., Sokolov S.V., Tishchenko E.N., Shevchuk P.S. Cryptographic Protection of Information: A Tutorial. Moscow, 2025. (In Russ)
3. Shevchuk P.S., Zverev A.P., Pazin M.S. Ensuring Information and Cybersecurity of Military Personnel in the Digital Age During a Special Military Operation. *Engineering Bulletin of the Don*. 2025;11(131):. 934-945. (In Russ)
4. Dobot Yu.N., Shevchuk P.S. Botnet Attacks and Protection of Telecommunication Systems Using Cryptographic Methods. Innovative Potential for Science Development in the Modern World: Achievements and

Innovations: Collection of Scientific Articles Based on the Proceedings of the XV Int. Res. and Pract. Conf. – Ufa, 2024:11–18. (In Russ)
5. Dobot Yu.N., Shevchuk P.S. Detection and Mitigation of DDoS Attacks Based on SIEM // Innovative Ideas of Young Researchers: Collection of Scientific Articles Based on the Materials of the XV International Scientific and Practical Conf. – Ufa, 2024; 29–34. (In Russ)
6. Federal Law of the Russian Federation No. 152-FZ of 27.07.2006 (as amended on 06.02.2023) "On Personal Data". http://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 10.01.2026) (In Russ).
7. Plotkin A.S., Kesel S.A., Repin M.M., Fedorov N.V. Analysis of Vulnerabilities in Key Management Systems in Distributed Ledgers: The IBM Blockchain Case Study. *Cybersecurity Issues*. 2021; 2(42):61–70. (In Russ)
8. Petrov I.V., Sidorov A.A. Analysis of Vulnerabilities in Cryptographic Key Management Systems. *Cybersecurity Issues*. 2023; 4 (56):45–52. DOI: 10.21681/2311-3456-2023-4-45-52. (In Russ)
9. Ivanova M.S., Kozlov D.N. Challenges in Protecting Biometric Personal Data in Transport Infrastructure . *Information Security of Regions*. 2024;2 (47):18–25. (In Russ)
10. Livshits I.I. Risk Assessment of Personal Data Leakage from Supply-Chain Attacks. *Herald of Dagestan State Technical University. Technical Sciences.* 2025; 52(1):97–104. (In Russ)
11. Gruntovich M.M., Semkin A.N. Cryptographic Protection in the Support and Control System for Ground Vehicles*. Information Technology Security*. 2012; 19(1):65–69. (In Russ)
12. Gruntovskiy D.R., Sutorev I.S. Security Analysis of Containerized Applications in Environments with Special Data Security Requirements. *Modern Scientific and Technical Achievements: New Technologies, Innovative Solutions: Collection of Scientific Papers.* Ulyanovsk, 2025: 13–15. (In Russ)
13. Bokova O.I., Kanavin S.V., Khokhlov N.S., Gilev I.V., Lekar L.A. On Ensuring Secure Access to Information Systems Using Biometric Authentication Based on a Fuzzy User Identity Pattern and Neural Network Transformations. *Herald of Dagestan State Technical University. Technical Sciences*. 2023;50(4):. 75–84. (In Russ)
14. Cherkesova L.V., Savelyev V.A., Revyakina E.A., Polulyakh A.R., Sementsov M.A. Data Recovery Mechanism in the Event of Data Corruption, Infection, and/or Unauthorized Modification. *Herald of Dagestan State Technical University. Technical Sciences*. 2025;52(1):134–146. (In Russ)
15. Vasiliev A.E., Gazizov A.R., Shevchuk P.S. Cryptographic methods in access control systems: modern approaches and prospects. Actual problems of science and technology: materials of the All-Russian (national) scientific and practical conf., dedicated to the 95th anniversary of the Don State Technical University. - Rostov-on-Don, 2025; 383-384. (In Russ)
16. Smith J., Anderson K. Hierarchical Key Management Systems for Cloud Infrastructure. *Journal of Cryptographic Engineering.* 2023;13(3):245–258. – DOI: 10.1007/s13389-023-00312-5.
17. Chen L., Wang Y., Zhang H. Hardware Security Modules for Cryptographic Key Protection in Critical Infrastructure. *IEEE Transactions on Information Forensics and Security*. 2024;19:1234–1247. – DOI: 10.1109/TIFS.2024.1234567.
18. Johnson M., Brown R. Performance Analysis of AES-GCM for Biometric Data Protection. *Computers & Security*. 2023;134: Article 103421. – DOI: 10.1016/j.cose.2023.103421.
19. Smirnov V.I. Legal Aspects of Personal Data Protection in Information Systems: Monograph. – Moscow: Yurait, 2024; 284 p. (In Russ)
20. Davis P., Miller S. Cryptographic Agility in the Post-Quantum Era: Architectural Approaches. *ACM Computing Surveys*. 2024;56(2):Article 45. – DOI: 10.1145/3625567.
21. GOST R ISO/IEC 27001-2021. Information Technology. Security Techniques. Information Security Management Systems. Requirements. – Moscow: Standartinform, 2021. (In Russ)

Сведения об авторах:

Петр Сергеевич Шевчук, доктор технических наук, профессор кафедры информационной безопасности в вычислительных системах и сетях; andstyle@mail.ru

Айдинян Андрей Размикович, кандидат технических наук, доцент, доцент, кафедра информационной безопасности в вычислительных системах и сетях; 79081891239@yandex.ru; andstyle@mail.ru; ORCID: 0000-0001-9455-4079

Information about the authors:

Petr S. Shevchuk, Dr. Sci. (Eng.), Prof., Department of Information Security in Computing Systems and Networks; andstyle@mail.ru

Andrey R. Aidinyan, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department of Computing Systems and Information Security, 79081891239@yandex.ru; andstyle@mail.ru ORCID: 0000-0001-9455-4079

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 19.10.2025.

Одобрена после рецензирования/Reviced 11.01.2026.

Принята в печать/ Accepted for publication 12.04.2026.