УДК 004.02
DOI: 10.26102/2310-6018/2026.54.3.003

Метод восстановления биометрического ключа в доверенной среде исполнения и вывода локального сеансового ключа для защищенных операций на устройстве пользователя

В.В. Волхонский[1], И.В. Калиберда[2]✉, Е.А. Писаренко[3], С.Р. Василенко[3]

[1]Национальный исследовательский университет ИТМО, Санкт-Петербург, Российская Федерация
[2]Пятигорский институт (филиал) Северо-Кавказского федерального университета, Пятигорск, Российская Федерация
[3]Пятигорский государственный университет, Пятигорск, Российская Федерация

Резюме. Предложен метод локального восстановления биометрически создаваемого секретного ключа внутри доверенной среды исполнения с использованием помехоустойчивой криптографической конструкции типа извлекателя ключа и последующего вывода локального сеансового ключа. В архитектуре протокола явно различаются: (I) общий ключ защищенного канала связи, вычисляемый обеими сторонами исключительно из результата гибридного аутентифицированного установления общего секрета с постквантовым компонентом и транскрипта рукопожатия; и (II) локальный сеансовый ключ, вычисляемый только на клиентском устройстве внутри доверенной среды исполнения на основе результата локальной биометрической проверки. Локальный сеансовый ключ применяется для защиты локальных артефактов и выполнения критических операций на устройстве, не передается на сервер и не требуется для серверной проверки. Метод обеспечивает воспроизводимость при внутриклассовой вариативности биометрических измерений, минимизирует обработку биометрически обусловленного ключевого материала в информационной системе организации и реализует криптографически корректное разделение областей применения ключевого материала. Объектом исследования является внешний канал связи между терминалом пользователя и удаленным сервером компании; соединения между сервером компании, криптобиометрической системой и удаленной базой Единой биометрической системы, защищенные криптографическими средствами по государственным стандартам, рассматриваются как защищенные по допущению и не анализируются.

Ключевые слова: доверенная среда исполнения, биометрия, восстановление ключа, помехоустойчивое восстановление, функция вывода ключей, гибридное аутентифицированное установление ключей, постквантовое установление общего секрета, защищенный канал связи, транскрипт рукопожатия, удалённая идентификация.

Для цитирования: Волхонский В.В., Калиберда И.В., Писаренко Е.А., Василенко С.Р. Метод восстановления биометрического ключа в доверенной среде исполнения и вывода локального сеансового ключа для защищенных операций на устройстве пользователя. *Моделирование, оптимизация и информационные технологии.* 2026;14(3). URL: https://moitvivt.ru/ru/journal/article?id=2125 DOI: 10.26102/2310-6018/2026.54.3.003

Method for recovering a biometric key in a trusted execution environment and deriving a local session key for secure operations on a user's client device

V.V. Volkhonsky[1], I.V. Kaliberda[2]✉, E.A. Pisarenko[3], S.R. Vasilenko[3]

[1]National Research University ITMO, Saint Petersburg, the Russian Federation

[2]Pyatigorsk Institute (branch) of North Caucasus Federal University, Pyatigorsk, the Russian Federation
[3]Pyatigorsk State University, Pyatigorsk, the Russian Federation

Abstract. A method is proposed for locally recovering a reproducible biometric secret key within a trusted execution environment using an error-tolerant key-extraction construction, followed by deriving a local session key. The protocol architecture explicitly distinguishes: (I) a shared secure-channel key computed by both parties solely from the outcome of a hybrid authenticated shared-secret establishment procedure with a post-quantum component and the handshake transcript; and (II) a local session key computed only on the client device within the trusted execution environment based on the result of local biometric verification. The local session key is used to protect local artifacts and to perform critical on-device operations; it is neither transmitted to the server nor required for server-side verification. The method ensures reproducibility under intra-class variability of biometric measurements, minimizes server-side handling of biometric-derived key material within the organization's information system, and provides cryptographically sound separation of key-material domains. The object of study is the external communication channel between the user terminal and the company's remote server; inter-server links between the company server, the cryptobiometric system, and the remote database of the Unified Biometric System are assumed to be protected using certified cryptographic mechanisms compliant with national standards and are not analyzed.

Keywords: trusted execution environment, biometrics, key recovery, noise-tolerant recovery, key derivation function, hybrid authenticated key establishment, post-quantum shared-secret establishment, secure communication channel, handshake transcript, remote identification.

For citation: Volkhonsky V.V., Kaliberda I.V., Pisarenko E.A., Vasilenko S.R. Method for recovering a biometric key in a trusted execution environment and deriving a local session key for secure operations on a user's client device. *Modeling, Optimization and Information Technology*. 2026;14(3). (In Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2125 DOI: 10.26102/2310-6018/2026.54.3.003

Введение

В задачах удаленного доступа в информационные системы организации биометрия рассматривается как удобный фактор подтверждения присутствия пользователя. Однако биометрические данные характеризуются вариативностью повторных измерений и повышенными рисками при обработке и хранении. В российской правовой модели идентификации и аутентификации с использованием биометрических персональных данных существенную роль играет централизованный контур (Единая биометрическая система) и ограничения на обработку биометрических данных вне этого контура, что делает архитектурно важным принцип минимизации биометрических артефактов в информационных системах организаций[1].

Параллельно усиливаются требования к долговременной криптографической стойкости защищенных каналов в условиях угрозы типа «записать сейчас – расшифровать потом». Объектом исследования в настоящей работе является внешний канал связи между терминалом пользователя и удаленным сервером компании, включая процедуры установления защищенного соединения, вывода ключевого материала и передачи биометрического представления (bestshot) по данному каналу. Взаимодействие удаленного сервера компании с удаленным сервером компонента криптобиометрической системы и удаленной базой биометрических персональных

[1] Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации». Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru/novye-postupleniya/federalnyy-zakon-ot-29-12-2022-572-fz-ob-osushchestvlenii-identifikatsii-i-ili-autentifikatsii-fizich/?sphrase_id=14017 (дата обращения: 25.09.2025).

данных Единой биометрической системы осуществляется по выделенным защищенным межсерверным соединениям с применением криптографической защиты по государственным стандартам; указанные соединения рассматриваются как защищенные по допущению и не входят в область исследования и анализа в рамках данной статьи.

Вариативность биометрических измерений и невозможность их точного воспроизведения при повторных съемах обусловливают необходимость применения помехоустойчивых криптографических методов восстановления секретов, формализованных в моделях fuzzy extractor и secure sketch, получивших развитие в ряде последующих работ [1, 2].

В современных исследованиях также рассматриваются архитектурные подходы, направленные на повышение конфиденциальности биометрических данных за счет их преобразования и распределенной обработки. В частности, предлагаются схемы отменяемой биометрии (cancelable biometrics) в сочетании с федеративным обучением, позволяющие снизить риски компрометации биометрических шаблонов без существенного ухудшения точности аутентификации [3]. Параллельно исследуются методы выполнения биометрической проверки над зашифрованными представлениями с применением гомоморфного шифрования и траншифрования, обеспечивающие приватность биометрических данных на всех этапах обработки [4]. Кроме того, предлагаются протоколы биометрической аутентификации, в которых подтверждение личности достигается без раскрытия биометрического шаблона сервис-провайдеру, что дополнительно усиливает аргументацию в пользу приватной обработки биометрических данных [5].

Это стимулирует использование постквантовых механизмов установления общего секрета (в частности, стандартного механизма инкапсуляции ключа на модульных решетках)[2]. Вместе эти факторы формируют потребность в методе, который связывает факт локальной биометрической проверки с выполнением критических операций на устройстве, не превращая биометрию в сетевой секрет или серверный фактор.

Цель настоящей работы – описать завершенный метод, в котором:

1) биометрия используется только локально внутри доверенной среды исполнения для воспроизводимого получения секрета K_{bio}[3] [1];

2) общий ключ канала K_{chan} формируется только из результата постквантового установления секрета K_{pqc} и транскрипта рукопожатия[2,4];

3) локальный ключ K_{sess}^{loc} связывает защищенный канал с фактом локального «user verification», не создавая серверной зависимости от биометрических производных[5,6].

Материалы и методы

Постановка задачи. Требуется построить механизм, который при каждом сеансе доступа:

– выполняет локальную биометрическую проверку пользователя;

---

[2] FIPS 203. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Gaithersburg: NIST; 2024. 47 p. https://doi.org/10.6028/NIST.FIPS.203

[3] ISO/IEC 24745:2022. *Information security, cybersecurity and privacy protection – Biometric information protection.* Geneva: ISO; 2022. 63 p.

[4] Rescorla E. *The Transport Layer Security (TLS) Protocol Version 1.3: RFC 8446.* IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата обращения: 25.09.2025).

[5] Krawczyk H., Eronen P. *HMAC-based Extract-and-Expand Key Derivation Function (HKDF): RFC 5869.* IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc5869 (дата обращения: 25.09.2025).

[6] Barker E., Chen L., Davis R. *NIST Special Publication 800-56C. Rev. 2. Recommendation for Key-Derivation Methods in Key-Establishment Schemes*. Gaithersburg: NIST; 2020. 33 p. https://doi.org/10.6028/NIST.SP.800-56Cr2

– восстанавливает внутри доверенной среды исполнения одинаковый (воспроизводимый) секрет K_{bio} при условии близости повторного биометрического шаблона к эталонному;

– выводит локальный ключ K_{sess}^{loc}, зависящий от K_{bio} и K_{pqc}, но не требующий вычисления на сервере и не передаваемый ему.

Подобная постановка задачи соответствует современным подходам к локальной биометрической аутентификации, в которых биометрия используется исключительно как фактор пользовательской верификации (user verification), а не как сетевой аутентификационный секрет, что подчеркивается как в работах по защищенным вычислениям и доверенным средам исполнения[7] [6], так и в исследованиях, ориентированных на приватную обработку биометрических данных и минимизацию их раскрытия в распределенных и зашифрованных вычислительных средах [3, 4]. Практическая реализуемость подобной архитектуры дополнительно подтверждается решениями, в которых терминальные доверенные среды исполнения сочетаются с защищенными серверными компонентами и механизмами пользовательского контроля над биометрическими данными [7].

Модель угроз. Рассматривается противник, способный реализовать полный контроль над внешним каналом связи «терминал пользователя – удаленный сервер компании» (перехват, модификация, повтор, задержка и переупорядочивание сообщений), а также способный контролировать прикладную среду терминала вне доверенной среды исполнения. При этом предполагается, что код, исполняемый в доверенной среде исполнения, корректно изолирован от недоверенной операционной системы и использует защищенные механизмы хранения (sealed storage) и управления жизненным циклом секретов.

В рамках рассматриваемой модели противника основными целями атак являются: (I) нарушение конфиденциальности и целостности передаваемого bestshot; (II) подмена контекста рукопожатия и параметров сессии; (III) атаки повтором на протокол установления ключей; (IV) попытки индукции отказа и истощения (rate/attempt exhaustion) на стороне терминала. Противодействие данным угрозам достигается (а) привязкой вывода общего ключа защищенного канала к транскрипту рукопожатия и контексту сессии, и (б) локальным выполнением биометрически обусловленных операций только внутри доверенной среды исполнения с политиками ограничения попыток[7].

Указанная модель противника и допущения об изоляции доверенной среды исполнения соответствуют принятой в литературе модели угроз для TEE-архитектур, используемых в системах удаленной аутентификации и защищенного хранения ключевого материала[7,8].

Сценарий применения и архитектура взаимодействия. Рассматривается сценарий удаленной идентификации сотрудника для получения доступа в информационную систему компании. Архитектура включает следующие логические компоненты: терминал пользователя с сенсорами получения изображения лица в спектральных каналах RGB и LWIR (тепловизионный используется только для подтверждения живого присутствия человека); удаленный сервер компании; удаленный сервер компонента Коммерческой биометрической системы (КБС), выполняющий сопоставление с векторными представлениями; удаленная база биометрических персональных данных

[7] GlobalPlatform Technology. *TEE System Architecture – Public Release v1.3. GPD_SPE_009.* GlobalPlatform; 2011–2022. 78 p.
[8] Costan V., Devadas S. *Paper 2016/086. Intel SGX Explained.* Cryptology ePrint Archive. URL: https://eprint.iacr.org/2016/086 (дата обращения: 28.09.2025).

Единой биометрической системы (ЕБС), используемая в контуре криптобиометрической системы. При этом внешний защищенный канал устанавливается только между терминалом пользователя и удаленным сервером компании и является объектом исследования; взаимодействие между сервером компании, сервером криптобиометрической системы и базой ЕБС осуществляется по межсерверным соединениям, защищенным по государственным стандартам, и рассматривается вне рамок исследования (Рисунок 1).

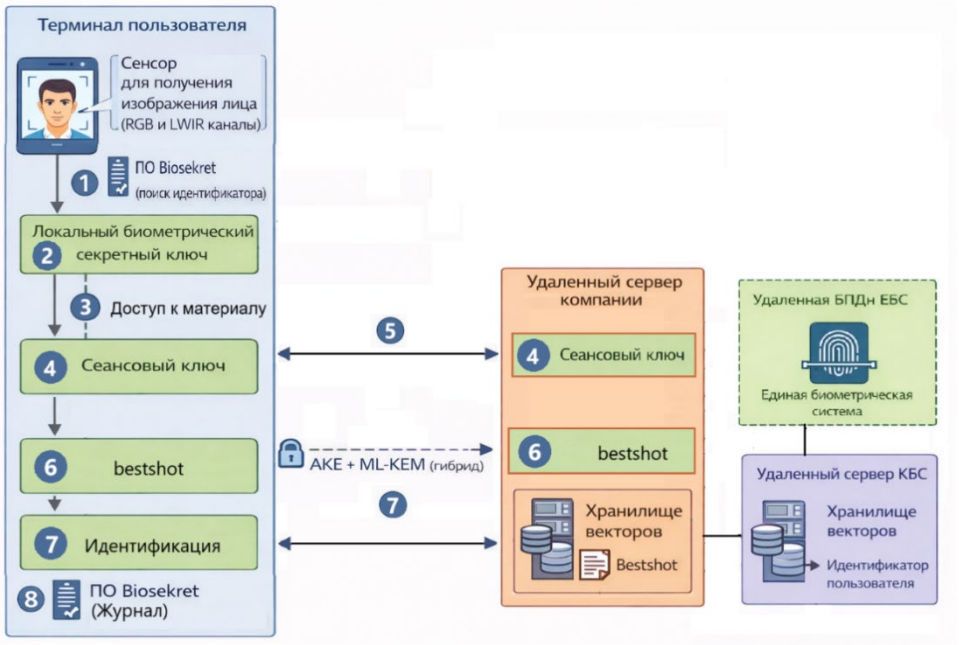

Рисунок 1 – Схема удаленной идентификации сотрудника для получения доступа в информационную систему компании
Figure 1 – Remote employee identification scheme for gaining access to the company's information system

Последовательность взаимодействий включает следующие этапы. При инициировании запроса на идентификацию терминал выполняет локальную обработку биометрии. Полученный идентификатор используется терминалом для обращения к программному обеспечению Biosekret, в котором осуществляется поиск данного идентификатора в локальной базе (шаг 1). При наличии совпадения формируется заключение об успешной идентификации и формируется биометрически воспроизводимый секретный ключ (шаг 2). Далее данный ключ используется для контролируемого доступа к сеансовому ключу, предназначенному для локальной защиты артефактов и критических операций на терминале (шаг 3). После терминал и удаленный сервер компании выполняют стандартный протокол аутентифицированного установления ключей, дополненный постквантовым механизмом инкапсуляции ключа (гибридная схема), в результате чего формируется общий ключ защищенного канала связи для обмена сообщениями (шаг 4).

По установленному защищенному каналу терминал передает на удаленный сервер компании отобранный кадр наилучшего качества (bestshot) (шаг 5). Сервер компании, действуя в рамках организационного контура и разграничения доменов обработки, перенаправляет bestshot на удаленный сервер, функционирующий под управлением компонента КБС, где выполняется сопоставление поступившего представления с ранее выгруженными векторами (шаг 6). В случае успешного

сопоставления сервер КБС формирует и передает на терминал пользователя идентификатор (номер) найденной записи (шаг 7). Завершающим этапом является регистрация результата идентификации в журнале мониторинга программного обеспечения Biosekret для целей аудита и последующего контроля (шаг 8).

Таким образом, криптографическая защита внешнего канала «терминал – сервер компании» обеспечивает конфиденциальность, целостность и связность контекста передачи bestshot и результатов идентификации, тогда как биометрически обусловленный ключевой материал и операции с ним локализованы в доверенной среде исполнения терминала и не используются для вычисления общего ключа канала и не передаются на сервер.

Преобразование шумных источников (включая биометрию) в криптографически пригодный ключ формализовано в конструкциях fuzzy extractor и secure sketch, обеспечивающих воспроизводимость и (почти) равномерность извлеченного секрета при наличии вспомогательных данных [1]. Для сценариев, где требуется устойчивость к активным воздействиям и привязка к протоколам согласования ключей, разработаны robust-варианты fuzzy extractor и схемы аутентифицированного согласования из «близких секретов» [8].

Требования к защите биометрической информации (в том числе необратимость и несвязываемость) и принципы минимизации хранимых артефактов систематизированы в ISO/IEC 24745[3]. Для постквантового установления общего секрета используем стандартную постановку механизма инкапсуляции ключа; модульно-решеточный стандарт описан в FIPS 203[2]. Для вывода ключей из исходного общего секрета применяются рекомендации HKDF и норматива по методам key derivation в схемах установления ключей[5,6]. Привязка ключевого материала к транскрипту рукопожатия является общим принципом современных протоколов защищенного транспорта (например, TLS 1.3)[4].

Математическая модель биометрического шаблона. Пусть результат захвата лица пользователя представлен эмбеддингом:

$$X \in \mathbb{R}^d, \tag{1}$$

где d – размерность признакового пространства.

Повторные измерения одного и того же пользователя при корректном предъявлении образуют выборки:

$$X, X' \sim D_{user}, \tag{2}$$

где D_{user} – распределение внутриклассовой вариативности биометрического признака конкретного пользователя.

Для помехоустойчивой криптографической обработки применяется детерминированная функция бинаризации (квантизации):

$$Q: \mathbb{R}^d \to \{0,1\}^n, \tag{3}$$

в результате которой формируются бинарные шаблоны:

$$w = Q(X), \tag{4}$$

$$w' = Q(X'). \tag{5}$$

Предполагается существование порогового значения t, такого что при корректном съеме и отсутствии атак предъявления выполняется условие близости:

$$\mathrm{dist}_H(w, w') \leq t, \tag{6}$$

где $\mathrm{dist}_H(\cdot,\cdot)$ – расстояние Хэмминга. Данная постановка соответствует модели «близких секретов» и является стандартной для применения помехоустойчивых криптографических конструкций типа fuzzy extractor.

Использование расстояния Хэмминга и пороговой модели близости бинарных шаблонов является стандартным подходом при построении биометрических криптосистем и подтверждено как в теоретических, так и в прикладных исследованиях [2, 9]. Функции извлечения эмбеддингов и квантизации $Q(\cdot)$ фиксируются по версии и не изменяются без процедуры повторной регистрации, поскольку их модификация нарушает воспроизводимость бинарных шаблонов и приводит к росту вероятности отказа восстановления [1, 8].

Конструкция (Gen, Rep) и восстановление биометрического секрета в доверенной среде исполнения.

Используемая помехоустойчивая конструкция. Для восстановления биометрически воспроизводимого секрета используется реализация fuzzy extractor на основе схемы code-offset с линейным исправляющим кодом. Обозначим функции кодирования и декодирования:

$$\mathrm{Enc}:\{0,1\}^l \to \{0,1\}^n, \quad \mathrm{Dec}:\{0,1\}^n \to \{0,1\}^l \cup \{\perp\}. \tag{7}$$

где l – длина внутреннего секрета, а $\perp$ обозначает отказ восстановления.

Исправляющий код корректно восстанавливает исходный секрет при числе ошибок, не превышающем t.

Фаза регистрации (Enrollment): алгоритм Gen. Внутри доверенной среды исполнения выполняются шаги:

1. Съем и предварительная проверка.

Выполняется детекция и выравнивание лица, контроль качества и, при необходимости, проверка живости. Данные этапы направлены на снижение вероятности ошибок восстановления и противодействие атакам предъявления[9].

2. Формирование бинарного шаблона.

По результату съема вычисляется w по формуле (4).

3. Генерация случайного секрета:

$$R \xleftarrow{S} \{0,1\}^l. \tag{8}$$

4. Кодирование секрета:

$$\mathrm{c} = \mathrm{Enc}(R) \in \{0,1\}^n. \tag{9}$$

5. Формирование вспомогательных данных (helper data):

$$P_{loc} = c \oplus w. \tag{10}$$

6. Нормализация биометрического секрета. В предлагаемом методе для нормализации восстановленного биометрического секрета и формирования ключевого материала используется стандартная схема «извлечение-расширение» (HKDF), реализуемая на базе криптографической хеш-функции «Стрибог» в соответствии с ГОСТ Р 34.11. На этапе расширения осуществляется вывод биометрического ключа:

$$K_{bio} = \mathrm{HKDF\text{-}Extract}(H(bio \parallel ctx), R), \tag{11}$$

[9] ISO/IEC 30107-3:2017. *Information technology – Biometric presentation attack detection. Part 3: Testing and reporting*. Geneva: ISO; 2017. 33 p.

где *ctx* – контекст доверенной среды исполнения, сериализованный в каноническом виде. HKDF используется как стандартный extract-шаг, обеспечивающий криптографически корректное получение ключевого материала из R[5].

7. Защищенное хранение. В доверенном хранилище сохраняются P_{loc} и параметры восстановления (версия пайплайна, параметры кода, политика попыток). Эмбеддинги X и бинарные шаблоны w долговременно не хранятся[3].

Фаза аутентификации (Session): алгоритм Rep. При очередном сеансе доступа внутри изолированной области процессора, обеспечивающей выполнение кода и защиту данных от остальной системы (TEE) выполняются следующие шаги.

1. Формирование текущего бинарного шаблона w' по формуле (5).

2. Восстановление зашумлённого кодового слова:

$$c' = P_{loc} \oplus w' = c \oplus (w \oplus w'). \tag{12}$$

3. Декодирование:

$$R' = \mathrm{Dec}(c'). \tag{13}$$

При $\mathrm{dist}_H(w, w') \le t$ выполняется $R' = R$; в противном случае, возвращается $\perp$, и локальная биометрическая проверка считается неуспешной [1].

4. Повторный вывод биометрического ключа:

$$K_{bio} = \text{HKDF-Extract}(H(bio \parallel ctx), R'). \tag{14}$$

Политики ограничения числа попыток и очистки промежуточных данных реализуются средствами TEE[7].

Применение линейных исправляющих кодов в схеме code-offset позволяет обеспечить баланс между устойчивостью восстановления и объемом вспомогательных данных, что подробно анализируется в ряде работ, посвященных практической реализации помехоустойчивых извлекателей ключей [9, 10].

Формирование ключей и разграничение контуров.

Общий ключ защищённого канала. В результате гибридного аутентифицированного установления ключей клиент и сервер получают постквантовый общий секрет K_{pqc}. Для его нормализации вводится:

$$PRK_{pqc} = \text{HKDF-Extract}(H(pqc \parallel tr \parallel ctx), K_{pqc}), \tag{15}$$

где *tr* – транскрипт рукопожатия.

Ключ защищенного канала вычисляется как:

$$K_{chan} = \text{HKDF-Extpand}(\text{PRK}_{pqc}, chan \parallel tr \parallel ctx, L_{chan}). \tag{16}$$

Привязка к транскрипту рукопожатия соответствует практике современных протоколов защищённого транспорта (в частности, TLS 1.3) и снижает риск атак типа unknown key-share и межпротокольных коллизий[4,6]. Важно, что K_{chan} не зависит от биометрии, и потому доступен обеим сторонам.

Локальный сеансовый ключ в доверенной среде исполнения. После успешного восстановления K_{bio} внутри TEE формируется смешанный псевдослучайный материал:

$$PRK_{mix} = \text{HKDF-Extract}(H(mix \parallel tr \parallel ctx), PRK_{pqc}, K_{bio}). \tag{17}$$

Далее:

$$K_{sess}^{loc} = \text{HKDF-Extract}(\text{PRK}_{mix}, loc \parallel tr \parallel ctx \parallel ver \parallel pol), L_{loc}), \tag{18}$$

где *ver* – версия биометрического пайплайна, а *pol* – идентификатор политики доверенной среды исполнения.

Ключ K_{sess}^{loc} существует только на клиентском устройстве и не передается серверу.

Подобное композиционное использование HKDF для вывода производных ключей из нескольких источников энтропии соответствует рекомендациям по построению многоуровневых схем управления ключами и широко применяется в современных протоколах защищённого взаимодействия[5] [11].

Использование этапов «извлечения и расширения» (extract-and-expand) в этой композиции соответствует роли HKDF как универсального механизма вывода ключей из исходного материала и рекомендациям по производному получению ключей в протоколах согласования ключей[5,6].

Использование локального сеансового ключа. Локальный ключ используется для защиты артефактов и операций на устройстве:

$$C = \text{AEAD.Enc}(K_{sess}^{loc}, token, aad = ctx). \quad (19)$$

Для отдельных операций выводятся специализированные ключи:

$$K_{op} = \text{HKDF-Extpand}(\text{PRK}_{mix}, op \parallel opid \parallel tr \parallel ctx, 32). \quad (20)$$

Такой режим обеспечивает привязку критических операций к факту локальной биометрической проверки и конкретному сеансу (через *transcript* и *ctx*), при сохранении принципов минимизации биометрических данных и несвязываемости серверных контуров[3].

Архитектурный принцип локализации биометрически обусловленного ключевого материала на стороне пользовательского устройства также согласуется с международными рекомендациями по privacy-by-design и снижению рисков корреляции биометрических данных между различными информационными системами[3,10], а также с современными научными подходами, в которых защита приватности достигается за счет исключения централизованного хранения биометрических шаблонов и выполнения биометрической проверки в доверенных или криптографически изолированных вычислительных средах [3, 4].

Корректность и параметры восстановления. Корректность восстановления обеспечивается свойствами исправляющего кода:

$$\text{dist}_H(w, w') \le t \Rightarrow R' = R. \quad (21)$$

Следовательно, K_{bio} воспроизводится, и K_{sess}^{loc} вычисляется детерминированно для данного сеанса при фиксированных K_{pqc}, *transcript* и *ctx* [1].

Вспомогательные данные P_{loc} предназначены для восстановления секрета при наличии близкого w' и не используется сервером. Ключевым требованием архитектуры является хранение P_{loc} в sealed-хранилище доверенной среды исполнения, что снижает риск утечек и корреляции между приложениями и соответствует принципам защиты биометрической информации, включая несвязываемость[3,7].

Компрометация сервера не раскрывает K_{bio} и K_{sess}^{loc}, так как они не покидают доверенную среду исполнения[7]. Общий ключ канала K_{chan} зависит только от K_{pqc} и *transcript* и соответствует криптографическим рекомендациям по derivation[5,6]. Устойчивость к многократным попыткам обеспечивается политиками rate limiting и блокировок в доверенной среде исполнения[7].

Регуляторная интерпретация (минимизация обработки биометрии). Метод не требует передачи на удаленный сервер компании биометрически обусловленного

[10] Единая биометрическая система. *Исследование российского и зарубежного рынка биометрических сервисов и биометрических платформ.* URL: https://ebs.ru/upload/iblock/df9/758uiix5u8nethuhvhlnu4h1mvbyjw72/Issledovanie-rynka-biometrii.pdf (дата обращения: 03.02.2026).

секретного ключа, вспомогательных данных извлекателя ключа, параметров восстановления и иных артефактов, позволяющих воспроизвести локальный ключевой материал. Передача биометрического представления (bestshot) по внешнему защищенному каналу рассматривается как прикладной этап идентификации и не используется для формирования общего ключа защищенного канала. Тем самым обработка биометрически обусловленного ключевого материала локализуется в доверенной среде исполнения терминала пользователя, а в серверном контуре отсутствует необходимость в хранении и обработке вспомогательных данных восстановления, что снижает риски компрометации и упрощает разграничение доменов обработки биометрической информации[1].

Результаты

Метод обеспечивает криптографически корректную привязку выполнения критических операций на устройстве к факту локальной биометрической проверки без передачи биометрических шаблонов, эмбеддингов и вспомогательных данных на сервер. Это снижает объем обработки биометрических данных в информационной системе организации и упрощает соблюдение ограничений на их обработку и хранение, установленных для информационных систем организаций при проведении аутентификации[1].

Результатом является воспроизводимый и управляемый механизм локальной защиты артефактов (токенов, контейнеров, ключей операций) в доверенной среде исполнения при сохранении стойкости канала на базе постквантового установления секрета[2].

Заключение

В результате исследования разработан метод, обеспечивающий локальную биометрическую проверку и восстановление биометрически воспроизводимого секретного ключа внутри доверенной среды исполнения с последующим выводом локального сеансового ключа, предназначенного для защиты локальных артефактов и выполнения критических операций на клиентском устройстве пользователя. Показано, что безопасность внешнего обмена сообщениями обеспечивается общим ключом защищенного канала, формируемым исключительно по результатам гибридного аутентифицированного установления ключей с постквантовой инкапсуляцией и привязкой к транскрипту рукопожатия и контексту сессии, без включения биометрически обусловленного компонента. Такой подход исключает необходимость передачи на сервер вспомогательных данных восстановления и иных биометрически зависимых секретов, снижая риски компрометации и упрощая доменное разделение обработки.

Объектом исследования является внешний канал связи «терминал пользователя – удаленный сервер компании»; межсерверные соединения «сервер компании – сервер криптобиометрической системы – база Единой биометрической системы», защищенные криптографическими средствами по государственным стандартам, рассматриваются как защищенные по допущению и не входят в область анализа.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Dodis Y., Ostrovsky R., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*. 2008;38(1):97–139. https://doi.org/10.1137/060651380

2. Juels A., Wattenberg M. A fuzzy commitment scheme. In: *CCS '99: Proceedings of the 6th ACM conference on Computer and communications security, 01–04 November 1999, Singapore.* New York: ACM; 1999. P. 28–36. https://doi.org/10.1145/319709.319714
3. Katkar V.D., Mandal R., Biswas U., et al. Enhancing biometric authentication privacy and security: A synergistic approach using cancelable biometrics and federated learning. *Alexandria Engineering Journal*. 2026;135:36–63. https://doi.org/10.1016/j.aej.2025.12.017
4. Yoo J.S., Ahn T.M., Yoon J.W. *Bidirectional Biometric Authentication Using Transciphering and (T)FHE.* arXiv. URL: https://arxiv.org/abs/2506.12802 [Accessed 3rd February 2026].
5. Guo Ch., You L., Li X., et al. A novel biometric authentication scheme with privacy protection based on SVM and ZKP. *Computers & Security.* 2024;144. https://doi.org/10.1016/j.cose.2024.103995
6. Bringer J., Chabanne H., Le Metayer D., Lescuyer R. *Biometric Systems Private by Design: Reasoning about privacy properties of biometric system architectures.* arXiv. URL: https://arxiv.org/abs/1702.08301 [Accessed 28th September 2025].
7. Sun Q., Wu J., Yu W. BioShare: An Open Framework for Trusted Biometric Authentication under User Control. *Applied Sciences.* 2022;12(21). https://doi.org/10.3390/app122110782
8. Dodis Y., Katz J., Reyzin L., Smith A. Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets. In: *Advances in Cryptology – CRYPTO 2006: 26th Annual International Cryptology Conference, 20–24 August 2006, Santa Barbara, CA, USA.* Berlin, Heidelberg: Springer; 2006. P. 232–250. https://doi.org/10.1007/11818175_14
9. Rathgeb Ch., Uhl A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security.* 2011;2011(1). https://doi.org/10.1186/1687-417X-2011-3
10. Boyen X. Reusable cryptographic fuzzy extractors. In: *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security, 25–29 October 2004, Washington, DC, USA.* New York: ACM; 2004. P. 82–91. https://doi.org/10.1145/1030083.1030096
11. Bellare M., Rogaway P. *Introduction to modern cryptography.* Boca Raton: CRC Press; 2005. 283 p.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Владимир Владимирович Волхонский, профессор, Национальный исследовательский университет ИТМО, Санкт-Петербург, Российская Федерация.
e-mail: volkhonski@mail.ru
ORCID: 0000-0001-9628-2046

Vladimir V. Volkhonskiy, Professor, National Research University ITMO, Saint Petersburg, the Russian Federation.

Калиберда Игорь Владимирович, старший преподаватель, Пятигорский институт (филиал) Северо-Кавказского федерального университета, Пятигорск, Российская Федерация.
e-mail: kaliberda-igor@yandex.ru
ORCID: 0000-0002-2792-9800

Igor V. Kaliberda, Senior Lecturer, Pyatigorsk Institute (branch) of North Caucasus Federal University, Pyatigorsk, the Russian Federation.

Писаренко Елена Анатольевна, доцент, Пятигорский государственный университет, Пятигорск, Российская Федерация.
e-mail: gmu41@yandex.ru
ORCID: 0000-0001-9086-386X

Elena A. Pisarenko, Associate Professor, Pyatigorsk State University, Pyatigorsk, the Russian Federation.

Василенко Станислав Романович, магистрант, Пятигорский государственный университет, Пятигорск, Российская Федерация.
e-mail: stanislav.r.vasilenko@gmail.com
ORCID: 0009-0000-1027-867X

Stanislav R. Vasilenko, Master's Degree student, Pyatigorsk State University, Pyatigorsk, the Russian Federation.

Статья поступила в редакцию 22.01.2026; одобрена после рецензирования 03.03.2026; принята к публикации 11.03.2026.

The article was submitted 22.01.2026; approved after reviewing 03.03.2026; accepted for publication 11.03.2026.